GUÍA DE CONTRATACIÓN DE SERVICIOS EN LA NUBE PARA EMPRESAS PÚBLICAS Y PRIVADAS EN COLOMBIA QUE GARANTICE UN CORRECTO ANÁLISIS FORENSE CUANDO SE PRESENTEN INCIDENTES DE SEGURIDAD

MARTHA CAROLINA PRECIADO BECERRA
MAGDA LUZ VARGAS HERRERA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE INFORMÁTICA
BOGOTÁ
2016

GUÍA DE CONTRATACIÓN DE SERVICIOS EN LA NUBE PARA EMPRESAS PÚBLICAS Y PRIVADAS EN COLOMBIA QUE GARANTICE UN CORRECTO ANÁLISIS FORENSE CUANDO SE PRESENTEN INCIDENTES DE SEGURIDAD

MARTHA CAROLINA PRECIADO BECERRA
MAGDA LUZ VARGAS HERRERA

PROYECTO DE GRADO

Asesor
ÁLVARO ESCOBAR ESCOBAR

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE INFORMÁTICA
BOGOTÁ
2016

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D. C., 26 de Noviembre del 2016

AGRADECIMIENTOS

Las autoras manifiestan agradecimiento y reconocimiento especial al ingeniero Álvaro Escobar Escobar por la orientación y colaboración brindada durante el proceso de investigación y desarrollo de la Guía.

También agradecen la participación del ingeniero Jhon Jairo Echeverri por su aporte en el inicio de la investigación.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVOS: “cualquier cosa que necesite protección por lo que representa para una empresa, frente a una situación de pérdida de la confidencialidad, integridad o disponibilidad”[1].

ANÁLISIS DE LOS RIESGOS: “proceso sistemático para identificar y estimar la magnitud del riesgo sobre un sistema de información”[2].

ANS: “acuerdos a niveles de servicio. Acuerdo escrito entre un proveedor de servicios y su cliente con el objetivo de fijar al nivel acordado de calidad de entrega de dicho servicio”[3].

ARTEFACTO FORENSE: “procesos o mecanismos de registro sobre toda actividad realizada por el sistema o el usuario, programas utilizados, accesos, conexiones, aplicaciones, descargas desde Internet, etc”[4].

CSP: cloud service provider: entidad u organización dedicada a proveer servicio y tecnología en infraestructura en la nube.

ENCARGADO DE TRATAMIENTO: “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”[5].

ISIRT: “equipo de respuesta a incidentes de seguridad de la información”[6].

[1] GESTIÓN CALIDAD. 2016. Definiciones: Seguridad de la Información SI: Activos. [En línea]. <http://gestion-calidad.com/definiciones-seguridad-informacion [citado en 7 de Septiembre de 2016].
[2] Ibíd., p. 5.
[3] SLA. S.f. Acuerdo de Nivel de Servicio. [En línea]. <http://asi-ut.bligoo.com.co/media/users/31/1555916/files/563120/Adsi_T3_Acuerdo_de_Nivel_de_Servicio_SLA.pdf>
[4] AREOS, Israel. 2015. Artefactos Forenses I. [En línea]. http://insecuredata.blogspot.com.co/2015/03/artefactos-forenses-i.html [citado en 17 de Marzo de 2015].
[5] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. S.F Glosario de términos. [En línea]. <https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php>
[6] SEARCH DATA CENTER. 2012. Equipo de Respuesta frente a incidentes de seguridad informática (CSIRT). [En línea]. <http://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT> [citado en Noviembre de 2012].

MALWARE: “software malicioso. Código de software informático cuyo objetivo es provocar daño a un sistema o causar mal funcionamiento”[7].

OFUSCACIÓN: “acción de encubrir un mensaje, haciéndolo difícil de entender”[8].

RIESGO: “es la posibilidad que una amenaza pueda causar cierto impacto negativo en un activo determinado que presenta una vulnerabilidad a dicha amenaza”[9].

TRATAMIENTO DE DATOS: “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, impresión, conservación, elaboración, evaluación, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”[10].

[7] RIVERO, Marcelo. S.f. ¿Qué son los Malwares? [En línea]. <https://www.infospyware.com/articulos/que-son-los-malwares/>.
[8] PÉREZ, Julián y GARDEY, Ana. 2012. Definición de Ofuscación. [En línea]. <http://definicion.de/ofuscacion/>.
[9] GESTIÓN CALIDAD. Op. cit., p. 2.
[10] CUIDA TUS DATOS. S.f. ¿Qué es un tratamiento de datos personales? [En línea]. <http://www.cuidatusdatos.com/infotratamiento.html>.

INTRODUCCIÓN

En la actualidad las nuevas tecnologías de la información proporcionan a las entidades y/o personas la posibilidad de migrar a plataformas que suministren una mayor disponibilidad, eficiencia e inmediatez de la información a bajos costos. Ante este panorama surgen tecnologías como **"**Cloud computing o información en la nube", que brinda características que buscan las empresas hoy en día, donde el manejo y la disposición de la información y aplicaciones es proporcionado por un tercero, sin que la compañía asuma costos de adquisición, administración y manejo de una infraestructura tecnológica que lo soporte.

Aunque los proveedores de servicio en la nube garantizan un alto grado de seguridad para el acceso y control de la información que manejan de sus clientes, aún hay incertidumbre ante cómo enfrentar un incidente que afecte el servicio o la seguridad de la compañía de forma legal y en la que se requiera un análisis forense digital, ¿Cómo será la cadena de custodia de la información?, ¿Qué leyes amparan el procedimiento?, ¿Quienes tendrán la potestad de autorizar un análisis forense en la nube?

En Colombia no se conoce hasta el momento ninguna norma o procedimiento definido que indique como realizar dicho análisis de los servicios informáticos en la nube.

Esta investigación propone una guía de contratación de servicios en la nube para empresas públicas y privadas en Colombia que garantice un correcto análisis forense cuando se presenten incidentes de seguridad teniendo en cuenta que en la actualidad no existe claridad sobre la correcta manipulación de la información que es compartida con los proveedores de servicios en la nube.

1. JUSTIFICACIÓN

En la actualidad se evidencia la falta de un procedimiento adecuado para la gestión de análisis forense de servicios contratados en la nube por las empresas en Colombia, ya que no hay claridad de la propiedad de los datos, del alcance en la manipulación de los datos y de la seguridad que debe ofrecer el proveedor en la custodia de los mismos.

No se conoce en Colombia la existencia de algún estándar o metodología en la cual las empresas públicas y privadas puedan tener como guía para la contratación de servicios en la nube, y en la cual se requiere involucrar aspectos de análisis forense en la atención de incidentes de seguridad. Se debe tener en cuenta que los procedimientos utilizados en un análisis forense en sistemas de cómputo tradicionales, difieren de los que se puedan realizar en un sistema en la nube.

La finalidad del presente trabajo busca desarrollar una guía, soportada por las leyes vigentes en Colombia, que le permitan a las empresas públicas y privadas realizar un contrato de servicios en la nube con empresas nacionales o internacionales, en el cual se contemplen los aspectos principales que amparen a la entidad y exijan al CSP llevar a cabo un correcto análisis forense en caso de que un incidente de seguridad lo requiera.

2. FORMULACIÓN DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

Responder a la siguiente pregunta ayuda a dar solución al problema jurídico que enfrentan las empresas en Colombia, cuando requieren contratar servicios en la nube, puesto que en el momento en que se presenten incidentes de seguridad, no es fácil tener el control en la investigación ya que la cadena de dependencias entre el proveedor de los servicios y los proveedores subcontratados puede llevar a la falta de coordinación entre todas las partes implicadas, lo cual llevaría a la imposibilidad de realizar Análisis Forenses adecuados.

¿La Guía de contratación ayuda a las empresas a Colombia a tener una mayor consideración de los problemas que enfrentan al momento de realizar un análisis forense ante incidentes de seguridad que se presenten en los servicios que han contratado en la nube?

2.2 OBJETIVO

2.2.1 Objetivo General. Elaborar una guía que ayude a las empresas públicas y privadas en Colombia a contratar de una manera adecuada servicios en la nube que garanticen un correcto análisis forense cuando se presenten incidentes de seguridad.

2.2.2 Objetivos Específicos.

- Investigar y analizar los aspectos legales vigentes en Colombia para la contratación de servicios en la nube.

- Formular recomendaciones para que las empresas en Colombia puedan realizar una adecuada contratación de servicios en la nube, teniendo en cuenta los aspectos necesarios para realizar un análisis forense en caso que se presente un incidente de seguridad.

- Identificar los principales riesgos que implica un inadecuado análisis forense en la nube.

- Elaborar un documento como guía que permita a las empresas públicas y privadas en Colombia, tener una referencia para contratar servicios en la nube

en el que se contemple un correcto análisis forense de un incidente de seguridad.

3. TIPO DE INVESTIGACIÓN

El tipo de investigación desarrollada con el presente trabajo es descriptivo, ya que en Colombia existen algunas leyes que contemplan figuras de protección jurídica para las empresas que contratan servicios en la nube, pero aún no hay una guía que le permita a las empresas considerar aspectos importantes a la hora de contratar dichos servicios.

4. HIPÓTESIS

4.1 HIPÓTESIS DE INVESTIGACIÓN

Se conocen las responsabilidades legales de los proveedores de servicios en la nube y de las empresas que contratan dichos servicios en Colombia, sobre la información que se transfiere a la nube. Así como la forma adecuada de realizar un correcto análisis forense.

4.2 HIPÓTESIS NULA

Se desconocen las responsabilidades legales de los proveedores de servicios en la nube y de las empresas que contratan dichos servicios en Colombia, sobre la información que se transfiere a la nube. Así como la forma adecuada de realizar un correcto análisis forense.

5. MARCO TEÓRICO

5.1 COMPUTACIÓN EN LA NUBE

El concepto de “computación en la nube” es una tecnología que se basa en el manejo de información en Internet, eliminando los costos asociados al almacenamiento, procesamiento y administración de los datos

¿Pero qué es Internet?, de acuerdo a la literatura se define como “un conjunto de ordenadores, distribuidos por el mundo y unidos por una tupida malla de comunicaciones, que ofrece espacios de información a todo el que tenga acceso”[11], a lo que llamamos nube.

La NIST (800-145) define la computación en la nube como: “un modelo que permite el acceso a la red omnipresente y conveniente a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que se puede aprovisionar y liberar rápidamente con un esfuerzo mínimo de gestión o una interacción entre el proveedor de servicios”[12].

De acuerdo con a la anterior definición la computación en la nube se describe como una tecnología flexible, que se adapta a las demandas de consumo, donde el usuario no conoce la infraestructura que lo soporta, los servicios son escalables y su nivel de interrupción es casi nulo.

El modelo de computación en la nube se compone de cinco características esenciales, tres modelos de servicio y cuatro implementaciones.

Las características más destacadas son:

- Escalable: el crecimiento va de acuerdo con las nuevas necesidades del usuario, sin que eso vaya asociado a nuevos contratos ni penalizaciones.

[11] MARTÍN, Eduardo. 2014. ¿Qué es ‘cloud computing’? Definición y concepto para neófitos. *TICbeat.* [En línea]. <http://www.ticbeat.com/cloud/que-es-cloud-computing-definicion-concepto-para-neofito> [citado en 2 de Diciembre de 2014].

[12] MELL, Peter y GRANCE, Timithy. 2014. The NIST Definition of Cloud Computing. *National Institute of Standards and Technology.* [En línea] <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [citado en 2014].

- Accesibilidad: por estar en internet permite un fácil acceso, no requiere estar ligado a una infraestructura, por lo contrario, ofrece la posibilidad del acceso a través de cualquier dispositivo (pc, teléfonos móviles, laptop).

- Recursos compartidos. La infraestructura que soporta la tecnología sirve a muchos usuarios de manera controlada y óptima, brindando seguridad en la asignación de recursos. Esto lleva inmerso un sin fin de recursos de almacenamiento, procesamiento, software, y hardware, los cuales son dispuestos para atender las necesidades por demanda de los usuarios, sin que estos tengan conocimiento de su topología y/o ubicación física.

- Reducción de costos: ya que no se invierte en infraestructura y los costos asociados a su operación y mantenimiento son trasladados, lo que disminuye sustancialmente la inversión en la administración.

- Seguridad: Es considerada aún más seguro que los sistemas tradicionales, ya que las empresas que ofrecen el servicio, destinan gran cantidad de recursos de infraestructura y de personal especializado dedicado a este aspecto.

5.1.1 Servicios Ofrecidos en la Nube. La computación en la nube ofrece una variedad de servicios en el que los usuarios y organizaciones acceden a través de una conexión de internet a una plataforma tecnológica dinámica (hardware, software), que permite desarrollar en este ambiente diferentes tareas entre las más nombradas se encuentran:

5.1.1.1 Software como Servicio SaaS. Bajo este modelo se encuentran aplicaciones con funcionalidades dirigidas a usuarios finales basados en la web o una interfaz del programa y las cuales son ejecutadas en la nube. Para su utilización es necesario la disponibilidad de ancho de banda, lo cual permite llegar a cualquier clase de organización. El consumidor no gestiona ni controla la infraestructura subyacente de la nube, incluida la red, servidores, sistemas operativos, almacenamiento o incluso capacidades de aplicación individuales, configuración limitada de aplicación específica del usuario[13].

[13] Ibíd., p. 1.

Entre sus características primordiales está su escalabilidad (crecimiento de acuerdo con las necesidades). Enfoque centralizado, en donde las actualizaciones benefician a gran cantidad de usuarios y, por último, es altamente parametrizable, lo que permite que los usuarios usen y vean lo que necesitan. Los mecanismos de seguridad y autenticación están bajo el control del proveedor, aunque en ocasiones la organización puede transferir este aspecto a otro tercero.

Las aplicaciones se utilizan a través de internet y los archivos se guardan en la nube, no en los ordenadores de los usuarios[14]. Las funcionalidades que se ofrecen en este tipo de servicios son soluciones back office, mensajería, gestión de correos electrónicos, antivirus, CRM y soluciones de integración.

5.1.1.2 Plataforma como Servicio PaaS. Proporciona una plataforma y un entorno que permite a los desarrolladores un despliegue de infraestructura que permite crear aplicaciones mediante la utilización de lenguajes de programación, bibliotecas, servicios y herramientas dispuestas con este fin, las cuales son administradas por el proveedor. El usuario tiene el control sobre las aplicaciones implementadas y ajustes sobre las mismas[15].

Los servicios se actualizan constantemente, mejorando funcionalidades y adicionando nuevas. También el servicio ofrece asesoría para el perfeccionamiento en las etapas del desarrollo hasta las pruebas e implementación.

Algunas herramientas que se proporcionan bajo esta plataforma son:

- Sistemas operativos.

- Entorno de script de servidor.

[14] ITU-T. 2014. Series y: Global information infraestructure, internet protocol aspects and next-generation networks. International Telecomunication Union. [En línea]. <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3502-201408-I!!PDF-E&type=items [citado en Agosto de 2014].
[15] MELL, Peter y GRANCE. Op. cit., p.1.

- Sistema de gestión de bases de datos.

- Soporte técnico.

- Almacenamiento.

- Herramientas de diseño y desarrollo.

- Hosting.

5.1.1.3 Infraestructura como Servicio IaaS. Bajo esta plataforma son proporcionados servicios en infraestructura de procesamiento, espacio en servidores virtuales, conexión de red, ancho de banda, hardware virtualizado y balanceo que le permite a la organización desplegar software de forma indeterminada. Esto incluye sistemas operativos y aplicaciones a los cuales el usuario tiene control, pero no a la infraestructura[16].

Las ventajas predominantes bajo esta plataforma son:

- Es altamente escalable. Las empresas pueden ampliar su infraestructura a medida que van creciendo, sin que se vea afectada la productividad de la organización.

- Costos adicionales de hardware. Ahorra costos de mantenimiento asociados a la infraestructura que soportará el servicio y de igual forma ahorro de tiempo de dedicación al mismo.

- No hay puntos únicos de falla. Si falla un componente de la plataforma que hace parte de la solución, el servicio no se verá afectado, debido a que la infraestructura es redundante.

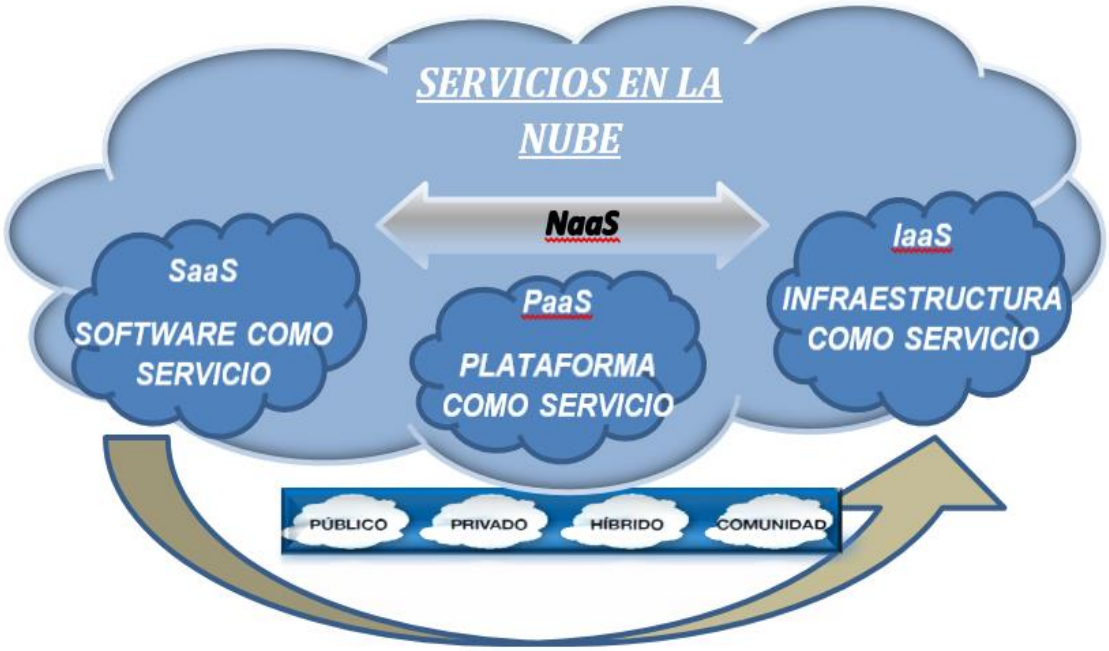
5.1.1.4 Red como servicio (Naas). Existen nuevos servicios que son catalogados bajo un ambiente de la nube como servicios de red (NaaS), que no es más que el control dinámico de la conectividad y gestión de red entre sistemas dentro del centro de datos de CSP, o entre sistemas de diferentes proveedores de servicios en la nube.

[16] Ibid.., p. 1.

Dentro de este enfoque se enmarcan funcionalidades como retardo limitado, jitter, ancho de banda, calidad de servicio, confiabilidad en todos los niveles y propósitos de la nube[17].

En la figura 1 se muestran las principales características de las plataformas en la nube.

Figura 1. Modelo de computación en la nube



Fuente: Elaboración propia.

5.1.2 Modelos de despliegue en la Nube. A continuación, se describen los diferentes modelos en que puede estar dispuesta los servicios en la nube, sus características más importantes.

5.1.2.1 Nube privada. Esta dispuesta para el uso exclusivo de una sola organización la cual está dispuesta por unidades de negocio, el cual puede ser administrados y operado por la organización, un tercero o su combinación y puede existir dentro o fuera de las instalaciones. Se tiene acceso a través de la web.

[17] ITU-T. Op. cit., p.1.

5.1.2.2 Nube Comunitaria. Esta dispuesta para el uso de una comunidad puede ser administrados y operado por una o más organizaciones de la comunidad, un tercero o su combinación y puede estar instalado dentro o fuera de las instalaciones.

5.1.2.3 Nube pública. Esta provista para uso abierto por el público en general. Puede ser operado por una organización comercial, académica u gubernamental o su combinación. Su infraestructura esta aprovisionada en centro de datos del proveedor.

5.1.2.4 Nube Hibrida. Está compuesta por dos diferentes infraestructuras, pública y privada, las cuales se entrelazan mediante tecnología lo que facilitan a las organizaciones flexibilidad.

5.1.3 Actores en la Nube. De acuerdo con la NIST, se define cinco actores dentro de un servicio en la nube[18]:

5.1.3.1 Consumidor de la nube. Persona u organización que mantiene la relación de negocios con el proveedor del servicio u intermediario y hace uso del mismo.

5.1.3.2 Proveedor de la nube. Persona u organización responsable de entregar el servicio disponible a las partes interesadas. Adquiere y administra la infraestructura de hardware y software necesario para ofrecer los diferentes servicios en la nube y a su vez brinda todo el desarrollo y despliegue de los mismos al usuario final.

5.1.3.3 Operador de la nube. Es el intermediario que ofrece conectividad y trasporte de los servicios entre proveedor y consumidor.

5.1.3.4 Auditor de la nube. Es la parte autorizada para realizar la evaluación del servicio, operación del sistema, rendimiento y seguridad de los servicios en la nube y entregar informes respecto a los hallazgos realizados durante la anterior actividad.

[18] LIU, Fang, et al. 2011. NIST Cloud Computing Reference Architecture. *National Institute of Standards and Technology.* [En línea]. <http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505> [citado en Septiembre de 2011].

5.1.3.5 Corredor de la nube. Es la entidad responsable de gestionar el uso, el rendimiento y la entrega del servicio. Es la parte que atiende las relaciones entre el proveedor de la nube y el consumidor. Brinda mejoras al servicio entregado, integrando funcionalidades o nuevos servicios.

5.2 GESTIÓN DE INCIDENTE

Para determinar un modelo de gestión de incidentes de seguridad se debe definir primero lo que es un evento y un incidente de seguridad.

5.2.1 Evento de seguridad. De acuerdo con la ISO 27001 se define como: "presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad"[19].

Se entiende entonces como evento cualquier alerta producto de una anomalía, o cambio de comportamiento en la infraestructura o componente de un sistema, el cual debe ser gestionado oportunamente antes que produzca un incidente de seguridad. De aquí la importancia del monitoreo de los componentes sensibles o vulnerables en la infraestructura.

5.2.2 Incidente de seguridad. De acuerdo con la norma ISO 27001 se denomina incidente de seguridad "un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información"[20].

Entendiendo de esta forma como incidente una violación a las políticas establecidas por una organización, que conlleve o atente contra la integridad, confidencialidad y disponibilidad de la infraestructura que hace parte del sistema de información y de la información misma.

La norma ISO 27001 del 2013, menciona de igual forma, los requerimientos para determinar, implementar, mantener y controlar un **Sistema de Gestión de**

[19] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. 2006. Tecnología de la información. Técnicas de seguridad. Sitemas de gestión de la seguridad de la información (SGSA). Requisitos. Bogotá: ICONTEC, 2006 (NTC-ISO/IEC 27001).
[20] Ibíd., p.11.

Seguridad de la Información como estrategia de toda organización, la cual debe estar alineada con los objetivos organizacionales con el fin de preservar los pilares de la seguridad de la información.

De la misma forma en el control A 16 de la misma norma, se define la Gestión de incidentes de Seguridad de la información como la acción de: "Asegurar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información sin excluir los eventos y debilidades"[21], y se mencionan los siguientes controles para la gestión de incidentes:

- Se debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada, a incidentes de seguridad de la información.

- Los eventos de la seguridad de la información deben ser reportados a través de los canales apropiados tan rápido como sea posible.

- Se debe exigir a los empleados y contratistas que usen los sistemas y servicios de información de la organización que tomen nota y reporten cualquier debilidad de seguridad de la información observada os sospechosa en sistemas o servicios.

- Los eventos en seguridad de la información deben ser evaluados y decidir si son clasificados como incidentes de seguridad.

- Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

- El conocimiento ganado del análisis y solución de incidentes de seguridad de la información debe ser usados para reducir la probabilidad e impacto de incidentes futuros.

- La organización debe definir y aplicar procedimientos para identificar, reunir adquirir y preservar información que pueda servir como evidencia.

[21] Ibíd., p.37.

5.2.3 ISO 27035 Gestión de Incidentes de la Seguridad Informática. Esta norma es un guía sobre el manejo de incidentes de seguridad en las organizaciones de forma estructurada y planificada, lo cual contribuye a:

- Mejora de la seguridad de la información.

- Reducir los impactos adversos para el negocio, ocasionados por los incidentes.
- Fortalecer el enfoque en prevención de incidentes de seguridad.

- Fortalecer la clasificación para la priorización de incidencias.

- Fortalecer los métodos y herramientas de recolección de evidencias.

- Justificación de inversión del presupuesto.

- Fortalecer las políticas de seguridad de la organización.

Para lograr este enfoque estructurado, la norma divide la gestión de Incidentes en las siguientes fases de acuerdo con la figura 2

Figura 2. Fases de la Gestión de Incidentes

Fuente: Elaboración propia.

Toda organización debe desarrollar una estrategia que dé cumplimiento al objetivo principal de la gestión de incidentes, la cual debe ir enfocada a evitar, detectar, contener y eliminar los incidentes de seguridad y así mismo minimizar, eliminar o asumir el impacto negativo de estos para la organización y relación a los costos directos e indirectos que se causen.

Para dar cumplimiento a los anteriores objetivos de la gestión de incidentes, se deben llevar a cabo cada una de sus fases expuestas en la figura 2.

La primera fase es la Planificación y preparación, en la cual se define las políticas de gestión de incidentes de seguridad de información, las cuales deben ser comunicadas a toda la organización. De igual forma en esta fase se plantea el establecimiento del equipo ISIRT (Equipo de respuesta a incidentes de seguridad de la información) y el grupo técnico y operativo para la atención a incidentes.

La segunda fase es la Detección y reportes, es la primera fase operativa de la estructura. Aquí se desarrolla un análisis de los perfiles de la ocurrencia de un evento y las vulnerabilidades del sistema. En la presente fase se llevará a cabo análisis de perfiles de tráfico, políticas de retención de bitácoras, sincronización de relojes y control de accesos a los sistemas e infraestructura.

La fase de Evaluación y decisiones categoriza los incidentes de acuerdo a los perfiles de los eventos analizados en la fase anterior y de acuerdo a esta actividad se determinará el impacto (físico, lógico) que pueden producir a la Confidencialidad, integridad y disponibilidad de la información.

La cuarta fase se denomina Respuesta a incidentes de seguridad de la información, de acuerdo a las acciones y tiempo de ejecución que fueron determinadas en la fase de evaluación y decisiones. Aquí serán tratado aspectos de análisis forense en caso de ser requerido; se definen estrategias de atención, contención, erradicación y recuperación ante un evento o incidente de seguridad.

La última fase de lecciones aprendidas, suma el aprendizaje y mejora del proceso, correlaciona incidencias, desarrolla mecanismos de retención de evidencias y evalúa el aprendizaje de los incidentes atendidos y el manejo de vulnerabilidades, con el fin del desarrollo de mejoras en cada una de las fases desarrolladas y permite la implementación de controles que permitan la mejora continua.

El numeral 8.2.5 de la norma habla sobre el análisis forense para la atención a incidentes que requieren este tipo de tratamiento. Esta actividad debe ser desarrollada por el ISIRT (Equipo de respuesta a incidentes de seguridad de la información), mediante el uso de técnicas y herramientas basadas en TI. Estos hallazgos deben ser documentados con el fin de que sirvan como evidencia en un proceso interno o legal.

5.3 ANÁLISIS FORENSE DIGITAL

El **análisis forense digital** es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnologías de punta para poder mantener la integridad de los datos y el procesamiento de los mismos, sino que también requiere de una experticia y conocimientos avanzados en materia de informática y sistemas, para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento no solamente del software sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información, etc.

5.3.1Metodología de Análisis Forense. La metodología empleada para el análisis forense se enumera a continuación:

- Identificar las fuentes donde se puede capturar la información de valor para la investigación.

- Realizar una correcta recolección de la información conservando su cadena de custodia, sin alterar los datos de origen.

- Se realiza una imagen de la información original, la cual es analizada documentando cada uno de los hallazgos obtenidos.

- Con los resultados anteriores se profiere un dictamen y unas conclusiones, las cuales servirán para la toma decisiones legales o correctivas, según sea el caso.

5.3.2 Análisis Forense en la Nube. El análisis forense en la nube, es la aplicación de análisis forense digital en la computación en la nube como un subconjunto de la ciencia forense de la red. Se trata de una disciplina transversal entre computación en la nube y análisis forense digital. De acuerdo con la definición oficial del NIST, “Digital Forensics es la aplicación de la ciencia a la identificación, análisis, recopilación y análisis de datos, mientras que la preservación de la información y el mantenimiento de una estricta cadena de custodia de los datos”.

Las tres dimensiones de la nube Forense:

- La dimensión técnica - Es un conjunto de herramientas y procedimientos necesarios para llevar a cabo el proceso forense en entornos de computación en la nube.

- La dimensión organizacional - en lo que respecta a las investigaciones forenses en entornos de computación en la nube, los dos partidos están siempre involucrados: el consumidor de la nube y el CSP. Cuando los CSP subcontratan a otras partes, hay una tendencia a que el alcance de la investigación se ensanche. Al establecer la capacidad de una organización para investigar las anomalías de la nube, cada organización debe crear un departamento encargado de los asuntos internos y externos que cumpla las siguientes funciones: investigadores, profesionales de TI, administradores de incidentes, asesores legales, y la asistencia externa.

- La cadena de dependencias - proveedores de servicios de nube y la mayoría de aplicaciones de la nube tienden a tener dependencias en otros CSP. Estas dependencias pueden ser altamente dinámicas, lo que significa que una investigación depende de cada eslabón de la cadena. Los problemas pueden derivarse de la interrupción o corrupción en cualquiera de los numerosos enlaces en la cadena o incluso debido a la falta de coordinación entre todas las partes implicadas. Por lo tanto, la comunicación y la colaboración entre las partes involucradas deben ser aplicadas por las políticas de la organización y legalmente vinculados a los SLAs.

A continuación, se describen los principales problemas que pueden afectar esta actividad en este ambiente:

1. Identificar los servicios y los proveedores de los mismos.

2. Imposibilidad de acceder a los medios físicos: Esta se puede dar por subcontratación de servicios, locación distribuida, recursos compartidos.

Por estos motivos, es recomendable, en este contexto no contemplar el acceso a medios físicos como un hecho, sino más bien derivar la tarea de recolección al proveedor del sistema. A su vez, sería deseable que el proveedor disponga de los

medios para poder obtener y aislar los datos para ser presentados al resto del equipo forense.

3. Información de clientes no relacionados: En el curso de una investigación esa información debe ser protegida y diferenciar claramente que pertenece a cada cliente y extraer como evidencia solo lo relacionado al cliente de la causa investigada. Esto también es una tarea que naturalmente recaería en el proveedor del servicio.

4. Interpretación del modelo de datos: Una vez adquiridos los datos, se debe disponer de algún medio de interpretación de los mismos. Nuevamente, recaería en el proveedor del servicio brindar la documentación necesaria para la correcta interpretación de los mismos, como por ejemplo modelos de datos, claves de encriptación, contexto semántico, conceptos del sistema, etc.

5. Sincronización horaria: Debido al alcance global de Computación en la Nube, un cliente podría estar utilizando servicio donde tanto los datos como los registros de sus acciones se encuentren en otro país, o continente, con una zona horaria distinta a él. Ante la presencia de un acto delictivo conocer la secuencia exacta de sucesos es crucial en la investigación.

6. Tercerización de servicios: Como se mencionó anteriormente éste sería el caso de un proveedor de un servicio que subcontrata otro proveedor de servicios.

Dadas estas problemáticas en la informática forense en la nube, es posible notar que la participación y la dependencia del proveedor del servicio es crucial para el desarrollo de una investigación. De no contar con ello, adquirir, obtener y preservar los datos sería extremadamente difícil. Por ello es necesario que en los Términos y Condiciones del Servicio (SLA) estén pactadas las obligaciones relacionadas con las disponibilidad y recuperación del acceso a la información.

También es necesario contar con acuerdos que habiliten a peritos informáticos los medios para solicitar a los proveedores dicha información. Estos acuerdos, idealmente, deberían ser internacionales ya que dado el alcance global de los servicios de computación en la nube es posible que el cliente y el proveedor pertenezcan a diferentes países.

5.4 CONTROLES Y LEGISLACIÓN

Como parte de la investigación se tomaron varios trabajos realizados sobre el aspecto legal de los servicios contratados en la nube y la jurisdicción que los rige.

Las aplicaciones de nube en el sector público y privado comprenden la posibilidad de trastear de la tierra a la nube los datos personales de empleados, clientes y ciudadanos en general. Estos pueden ser almacenados, procesados y administrados por empresas que proveen servicios de nube (CSP). Lo que se haga o no con la información dependerá del contrato que se suscriba.

5.4.1 Análisis Legal de Computación en la Nube. La descripción teórica de la Computación en la Nube, sus características, esquemas comerciales de ofertas de servicio y tipos de nube evidencian que se trata de una nueva forma de aproximación a la manera en que las personas naturales y jurídicas almacenan información y la comparten. Frente a este fenómeno en el cual los ordenamientos jurídicos deben ser interpretados y actualizados con el fin de identificar los cuestionamientos o incertidumbres legales que puedan surgir.

Es por esto que el estudio de la computación en la nube debe empezar en la naturaleza legal del servicio y los retos jurídicos que se presentan sobre este tipo de contratos.

5.4.2 Derecho Comparado. Consiste en el estudio de las diversas instituciones jurídicas a través de las legislaciones positivas vigentes en distintos países.

Dentro de las consideraciones legales también es importante tener claro el concepto del derecho comparado**,** ya que es necesario realizar un estudio de las diversas instituciones jurídicas a través de las legislaciones positivas vigentes en distintos países.
El derecho comparado se debe enfocar a la investigación restringida a legislaciones de similar afinidad cultural[22].

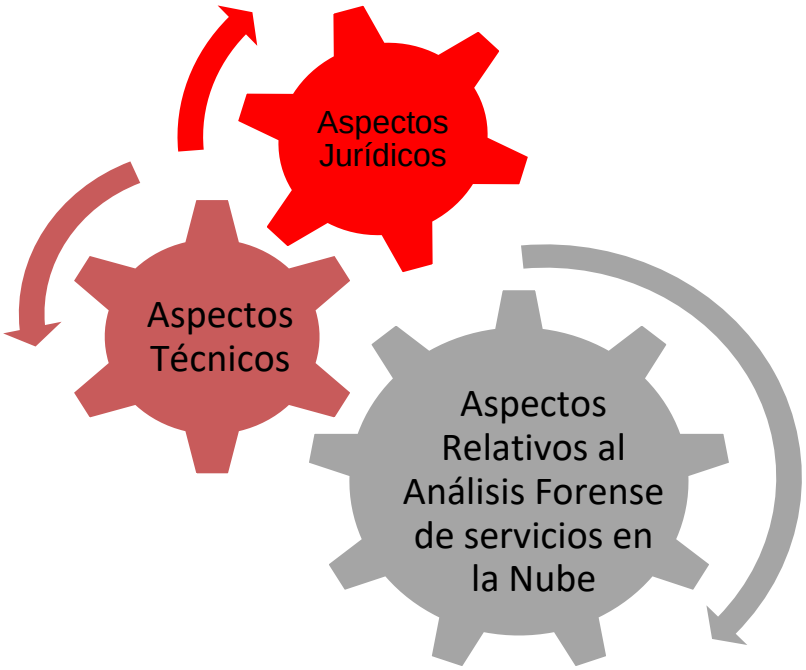
[22] ENCICLOPEDIA JURÍDICA. S.f. Derecho comparado. *Enciclopedia jurídica.* [En línea]. <http://www.enciclopedia-juridica.biz14.com/d/derecho-comparado/derecho-comparado.htm> [citado en S.f].

6. GUÍA DE CONTRATACIÓN DE SERVICIOS EN LA NUBE PARA EMPRESAS PÚBLICAS Y PRIVADAS EN COLOMBIA QUE GARANTICE UN CORRECTO ANÁLISIS FORENSE CUANDO SE PRESENTE INCIDENTES DE SEGURIDAD

En el presente capítulo se darán las recomendaciones a tener en cuenta al momento de la contratación de servicios en la nube que garanticen un adecuado manejo para el análisis forense en el momento en que se presente un incidente de seguridad, basados en las normas ISO 27037, ISO 27042 y de la NIST 8006, así como las leyes vigentes de contratación y protección de datos en Colombia.

Para ello se abordar tres diferentes aspectos que se deben considerar en toda contratación de servicios en la nube, los cuales se constituyen en un engranaje y se complementan entre sí, como se observa en la figura 3.

Figura 3. Aspectos Relativos a la contratación en la nube



Fuente: Elaboración propia.

6.1 ASPECTOS JURÍDICOS

Los mayores retos a nivel jurídico en este tipo de contratación, se presentan en la protección de datos personales, la transferencia internacional de datos, la seguridad de la información almacenada en la nube, las actuaciones criminales, la responsabilidad civil, etc. y el problema de la ley que se debe ser aplicada a este tipo de contratos y bajo qué jurisdicción se encuentran.

A continuación, se describen las recomendaciones en el aspecto jurídico a tener en cuenta para la contratación:

6.1.1 Definir las condiciones de la relación jurídica y la legislación que se aplica al momento de establecer un vínculo contractual. Teniendo en cuenta que la tecnología de computación en la nube permite a los proveedores ubicar los datos de los clientes en cualquier lugar del mundo. Por esta razón es necesario tener en cuenta los siguientes puntos:

> El cliente es responsable del trato de los datos, así haya contratado servicios de computación en la nube para su administración, por lo que la normativa aplicable al cliente y al prestador del servicio, debe garantizar la protección de los datos personales de los usuarios, conforme con las Leyes 1266 de 2008, Ley 1273 de 2009, como procedimientos para proteger la información personal. La cual se puede complementar con la Ley 1581 de 2012 (octubre 17) Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales. Siempre se deberá tener presente la Ley vigente de protección de información personal.
>
> El cumplimiento de las leyes no puede cambiarse contractualmente.
>
> Aunque informen que los datos personales están disociados, no cambia la ley aplicable ni la responsabilidad del cliente y del prestador del servicio[23].

[23] LEÓN VELANDIA, Beimar. 2014. *Metodología y recomendaciones para la contratación de servicios en la nube para empresas estatales en Colombia. Bogotá D.C, 2014, 156 h.* Tesis de investigación Magister en Ingeniería - Telecomunicaciones). Universidad Nacional de Colombia. Facultad de Ingeniería. Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial. Disponible en el catálogo en línea de la

6.1.2 Definir el lugar donde estará alojada la información. Necesario para dar un mejor manejo cuando se genere un incidente y se requiera la aplicación de ANS y/o se necesite el cumplimiento de los compromisos estipulados en el contrato.

> Debe recordarse que la Ley 1581 de 2012 sobre protección de información personal incorporó como prohibición la transferencia internacional de datos personales a países que no garanticen niveles adecuados de seguridad. Entendiendo que un país ofrece niveles adecuados cuando cumpla con los estándares de la Superintendencia de Industria y Comercio sobre la materia, las cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios, tal como lo señala el artículo 26 de la norma colombiana.[24]

Se considera que los países que cuentan con niveles adecuados de seguridad son los 28 países miembros de la Unión Europea, así como los países americanos que disponen de leyes de protección de datos personales, como Canadá, entre otros.

La figura contractual de la trasmisión internacional de datos personales existente en Colombia implica que los Responsables colombianos del tratamiento de datos personales sean conscientes que tales Encargados ubicados, particularmente en territorios no seguros, ofrezcan un nivel de protección equivalente al que se ofrece en Colombia[25].

> Debido a la complejidad de este tema la legislación colombiana aún no especifica los criterios que deben tenerse en cuenta para la transferencia internacional de datos. Por esta razón es necesario que el gobierno colombiano genere una legislación para regular la transferencia internacional de datos.
>
> Se debe preguntar al proveedor de servicios de computación en la nube si hay transferencias internacionales de datos y cuáles son las garantías.

Biblioteca de la Universidad Nacional de Colombia:<http://www.bdigital.unal.edu.co/46259/1/2707129.2014.pdf>.

[24] VELASCO & CALLE D´ALEMAN. 2016. Contratación en la Nube, Privacidad y recomendaciones de la Autoridad colombiana. (Parte 1). *Velasco & Calle D´Aleman.* [En línea]. <http://velascocalle.co/blog/contratacion-en-la-nube-privacidad-y-recomendaciones-de-la-autoridad-colombiana-parte-1/> [citado en 12 de Julio de 2016].

[25] LEÓN. Op., cit., p.48.

> Cuando los datos están localizados en terceros países podrá suceder que una Autoridad competente solicite y obtenga información sobre los datos personales de los que el cliente es responsable. En este caso el cliente debe ser informado por el proveedor de esta circunstancia (salvo que lo prohíba la ley del país tercero)[26].

6.1.3. Realizar el ejercicio del derecho comparado. En este tipo de contratación se hace necesario incluir el ejercicio del derecho comparado, el cual se debe enfocar a la investigación restringida a legislaciones de similar afinidad cultural[27].

Los objetivos del ejercicio de derecho comparado son:

- Unificación jurídica y también de armonización.

- Entendimiento internacional, porque nos hace comprender la razón de ser de las normas en los distintos estados.

- Un mejor conocimiento del derecho nacional, es decir, que utilizando el método comparativo se puede estudiar con mayor detalle los defectos legislativos y los aciertos legislativos.

Cuando se efectúa el ejercicio del derecho comparado, se adquiere un mayor conocimiento del derecho, porque se estudian las normas jurídicas dentro de diferentes sistemas jurídicos lo cual lleva a que se aumente la perspectiva.

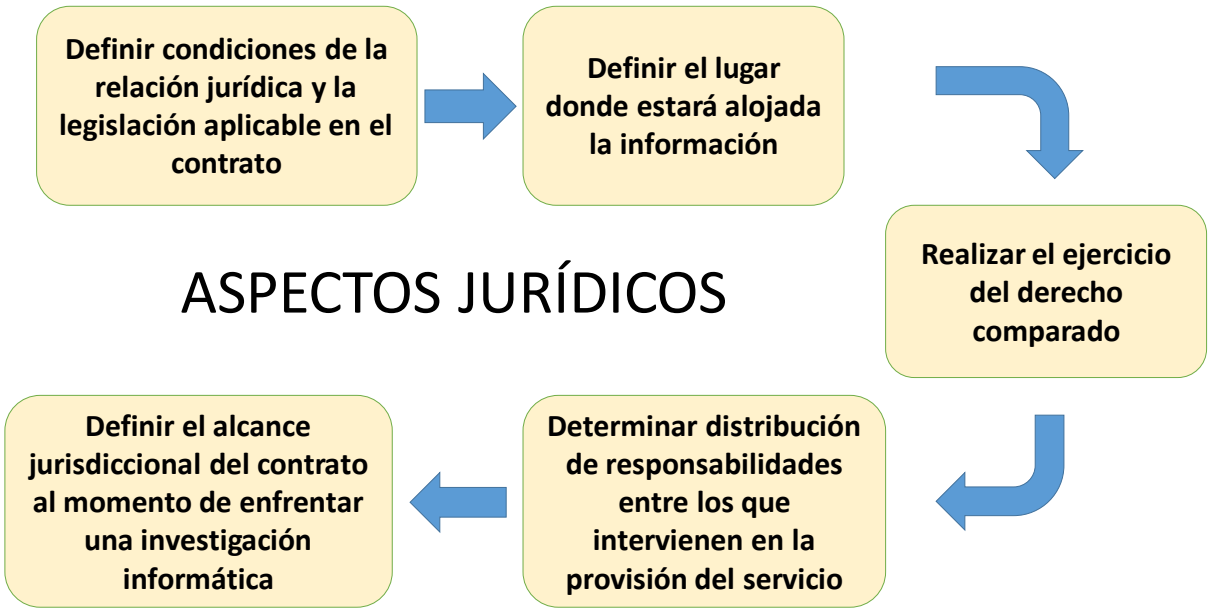
[26] Ibíd., p. 48.
[27] Ibíd., p. 1.

6.1.4 Determinar la distribución de responsabilidades entre los que intervienen en la provisión del servicio. Otro problema que se debe resolver en el momento de la contratación, es determinar la distribución de responsabilidades entre los que intervienen en la provisión del servicio al momento en que se requiera realizar una investigación forense. En un servicio puede haber un proveedor de la infraestructura física de la red (enrutadores, conmutadores, antenas, etc.), otro que disponga de los servidores que brinden espacio de almacenamiento y tiempo de procesamiento, otro que utilizando los servicios de los anteriores monte una plataforma de software como servicio; y así pueden seguirse generando diferentes proveedores según su contribución en la prestación. De esta manera, frente a la necesidad de realizar una investigación en un entorno tal, la actividad se vuelve compleja requiriendo determinar el nivel de participación que cada proveedor tiene en cada caso.

6.1.5 Definir el alcance jurisdiccional del contrato. Una vez se identifique la distribución de responsabilidades, el problema siguiente que enfrenta una investigación informática es el alcance jurisdiccional con que se puede contar. Generalmente se cuenta con apoyo legal a nivel de región dentro de un país; pero en esta gran red, los recursos se encuentran distribuidos a nivel internacional.

La figura 4, constituye los talantes más importantes a considerar en el aspecto jurídico.

Figura 4. Recomendaciones en el aspecto jurídico



Fuente: Elaboración propia.

6.2 ASPECTOS TÉCNICOS

Uno de los factores que se deben considerar en el momento de realizar un contrato de servicios en la nube, son los aspectos técnicos en el manejo de un incidente de seguridad, para ello es necesario determinar en primera instancia qué activos tiene la organización, y cuáles de ellos se llevan a la nube. Esto se debe realizar una vez se evalúe el nivel de riesgo asociado que conlleva para la organización, llevar cierta información a un ambiente fuera del ámbito empresarial, en donde el manejo, procesamiento y acceso a la misma será responsabilidad de un tercero.

A continuación, se describen los factores que se deben contemplar:

6.2.1 Identificar activos de información. Se define como activo de todos aquellos recursos que tiene valor para la organización y debe protegerse (hardware, software, instalaciones, servicios, personal). Los activos de información son aquellos recursos que la organización utiliza para el tratamiento de la información (bases de datos, servidores, impresoras, información licencias, equipos de comunicaciones).

De acuerdo con la norma ISO 27001, todas las organizaciones deben tener un inventario de los activos de información que será el punto de partida para desarrollar un adecuado análisis de riesgos que ayudará a determinar la criticidad del impacto para el negocio en caso de un fallo de seguridad sobre estos activos, que implique la pérdida de confidencialidad, integridad o disponibilidad de la información.

Aunque existen diferentes tipos de activos, los más importantes a considerar para llevar a la nube son:

- Activos de información como archivos, bases de datos, manuales de usuarios, documentación del sistema etc.

- Activos de software: aplicaciones, software de sistema, herramientas y programas de desarrollo.

- Activos físicos: equipos de cálculo, equipos de comunicaciones etc.

Una vez se establecen los activos de información, estos deben ser clasificados de acuerdo con su prioridad para el cumplimiento de los objetivos y misión organizacional. Se debe tener en cuenta en la clasificación de activos de información frente a la confidencialidad. Se puede tomar para ello la siguiente clasificación:

- Información pública: Es aquella que es de carácter público, y cuya divulgación no impacta a la organización y es accedida por personal interno y externo.

- Información de uso Interno: Es la que generalmente es compartida al interior de una organización con o sin autorización del dueño del activo.

- Información restringida: es de uso de un grupo limitado de persona de la organización y no debe ser difundida sin autorización.

- Información Confidencial: Es aquella que es de uso y conocimiento de los funcionarios de la organización y algunos terceros con los que se haya firmado previamente un acuerdo de confidencialidad. (datos personales, transacciones, actas directivas.).

Lo anterior será el punto de partida para identificar los activos de información que la organización pueda eventualmente llevar a la nube.

Se debe valorar las características de los datos teniendo en cuenta su mayor o menor sensibilidad.

Con esta información debe seleccionar el tipo de información para los cuales requiere contratar servicios de computación en la nube y cuales datos seguirá manejando en su propio datacenter. “Esta decisión es importante porque delimitará la finalidad que el proveedor de la nube aplicará a los datos. En consecuencia, debe garantizarse expresamente que no utilizará los datos para otra finalidad que no tenga relación con los servicios contratados” (España, 2013).

6.2.2 Análisis de Riesgos. Una vez identificados los Riesgos de la organización frente a los activos de información, se deben establecer los controles y mecanismos de seguimiento a los mismos.

Cada organización define la forma más apropiada para realizar la detección y evaluación de riesgos acorde al tipo de organización. Existen diferentes metodologías, normas y estándares disponibles entre las que encuentra Margerit 3, Octave, ISO 27005, RISK IT de ISAKA (basado en COBIT).

Existen diferentes clases de riesgos a los que se puede enfrentar la organización, entre los cuales están:

- Tecnológicos, provocados por fallas en el sistema o sus componentes.

- Riesgo interno o externo a la nube.

- Riesgo legal

- Riesgo de Acceso a la información

Cuando se desarrolla un análisis de riesgos de activos de información, se deben analizar todos aquellos riesgos presentes en una infraestructura tradicional, adicionalmente se deben considerar nuevos riesgos inherentes a los entornos en la nube, tales como los servicios vitalizados, arquitecturas orientadas a servicios o la web.

Para definir los riesgos asociados a un entorno en la nube se toma como referencia estudios realizados por organizaciones internacionales especializadas como la CSA Cloud Security Alliance, la agencia consultora Gartner, (empresa consultora y de investigación informática estadounidense) y la NIST. Estas entidades y grupos centran sus estudios y análisis en la protección de los principios básicos de la información confidencialidad, integridad y disponibilidad y otros factores relevantes como privacidad, la autenticación y aspectos como la ubicación de los datos. A continuación, se describen los puntos relevantes de cada una de ellas.

6.2.2.1 CSA: Cloud Segurity Alliance. La CSA se define como una organización internacional sin fines de lucro para promover el uso de mejores prácticas para garantizar la seguridad en cloud. En la tabla 1, se describen los riesgos que define la CSA respecto a los servicios en la nube.

Tabla 1. Riesgos de Acuerdo a CSA

RIESGO	ALCANCE
Abuso y uso nefasto de servicios cloud	Hace referencia al acceso no autorizado a plataformas de servicios IaaS y PaaS, con limitadas restricciones, con intensiones delictivas y dañinas, introduciendo spam o código malicioso
APIS Inseguras	Interfaces para acceder a los recursos e interactuar con los servicios en la nube poco seguros, exponiendo a los mismos a accesos anónimos, autenticaciones sin cifrar.
Hackeo de cuentas	Acceso de usuarios no autorizados para manipular datos, devolver información falsa, o re-direccionar a sitio maliciosos

Tabla 1. (Continuación)

RIESGO	ALCANCE
Ataques internos	Incidentes de seguridad ocasionados por error humano, desconocimiento u empleados descontentos, repercutiendo sobre los servicios que son administrados por el CSP.

Perdida de datos	Borrado o modificación de la información debido al número de interacciones propias de la arquitectura, ocasionando repercusiones económicas y problemas legales, cuando desemboca en una fuga de información
Riesgo de desconocimiento	Falta de conocimiento de infraestructura que soporta el servicio. Datos cómo con quién se comparte la infraestructura o los intentos de acceso no autorizados pueden resultar muy importantes a la hora de elegir la estrategia de seguridad. La carencia de información de este tipo puede derivar en brechas de seguridad desconocidas por el afectado.

Fuente: Elaboración propia.

6.2.2.2 GARTNER. Compañía especializada en tecnología de la información, investigación y consultoría a nivel mundial. Esta define los siguientes riesgos asociados a los servicios tecnológicos y de la información. Gartner define los riesgos que son especificados en la tabla 2.

Tabla 2. Riesgos de acuerdo a Gartner

RIESGO	ALCANCE
Acceso de usuarios con privilegios	Acceso a datos sensibles por ausencia de controles físicos, lógicos y humanos. Por lo anterior se debe limitar el acceso a los mismos a usuarios con privilegios.
Cumplimiento Normativo	Los contratantes de servicios en la nube son en última instancia los responsables de la seguridad e integridad de la información, en evento de una acción civil o penal.

Tabla 2. (Continuación)

RIESGO	ALCANCE
Aislamiento de datos	Los datos en la nube se encuentran en ambientes de datacenter compartidos con otros clientes; el CSP debe suministrar los

	mecanismos de cifrado seguro y fuerte**.**
Ubicación de datos	Desconocimiento de la ubicación de los datos. Por lo anterior es conveniente a incluir en los contratos y acuerdos un marco regulatorio para el almacenamiento y procesado de datos, adecuado al país del suscriptor del servicio.
Recuperación	El CSP debe contar con políticas que garanticen la recuperación de la información llevada a la nube, de manera oportuna y eficaz. Se debe contar con mecanismos de replicación de datos en diferentes infraestructuras.
Soporte Investigativo	Dificultad para adelantar investigaciones de actividades ilegales ya que los datos y logs se encuentran en información de diferentes clientes.
Viabilidad a largo plazo	Estabilidad del CSP en el mercado brindando servicio eficiente y eficaz. En caso de que sea comprado o adsorbido por un tercero se debe garantizar la disponibilidad, confidencialidad e integridad de la información

Fuente: Elaboración propia.

6.2.2.3 NIST. Instituto Nacional de Normas y Tecnología, cuya función primordial es promover la innovación y la competencia de los Estados Unidos mediante normas y tecnología. En la tabla 3 se relacionan los principales riesgos, especificados por la NIST.

Tabla 3. Riesgos de acuerdo a la NIST

RIESGO	ALCANCE
Gobernanza	Políticas, estándares y procedimientos de control para desarrollo, ejecución y la implementación del servicio en la nube. Es necesario poner en marcha un programa de

	riesgos flexible, con auditorias periódicas.
Cumplimiento	Está relacionada a la forma en que el CSP está alineado y opera de acuerdo a las políticas, leyes, regulación, del país vinculante. Esto puede constituirse un problema complejo, por aspectos como las regulaciones, localización de datos y aspectos de investigación electrónicas
Confianza	La organización cede el control en muchos aspectos de seguridad a el CSP y ello implica que este último cuente con rigurosos mecanismos de control de acceso por el personal interno; se estipule la propiedad de los datos y se tenga visibilidad de cómo se esa manejando la información y gestión de riesgo.
Arquitectura	Existen diferentes componentes en una arquitectura de servicios en la nube, las cuales operan a través de interfaces que son susceptibles a fallos de seguridad. Por lo anterior se debe tener en consideración las superficies de ataque, la protección interna de la red de servidores, y control de la penetración de código malicioso.
Identidad y control de acceso	Los CSP deben brindar una gestión de identidad y control de acceso que proporcionen garantías en la seguridad de la información. Mediante de mecanismos de identidad federada de acuerdo de estándar ya establecidos, mediante el empleo de mecanismos de autenticación y control de acceso.
Aislamiento de software	Los servicios de IaaS son susceptibles a ataques a las máquinas virtuales por cuenta de otro huésped que corre sobre un mismo servidor, por los anterior se hace necesario el aislamiento y aseguramiento de los diferentes componentes.

Tabla 3. (Continuación)

RIESGO	ALCANCE
Protección de Datos	Manejo, almacenamiento y procesamientos de datos sensibles. El CSP debe garantizar los mecanismos de protección de estos datos y saneamiento de la infraestructura utilizada.
Disponibilidad	Esta puede verse afectada temporal o permanentemente por fallos en la infraestructura que soporta la solución, ataques de DoS o desastres naturales.
Respuesta a Incidentes	El CSP debe tener estructurados la respuesta y atención de incidentes en todas sus etapas, verificación, análisis, contención, recolección de evidencias, solución del problema y restablecimiento del servicio

Fuente: Elaboración propia.

Se debe tener en cuenta el riesgo que representa para la organización colocar los datos o transferir cada uno de los activos de información a un entorno compartido con otras organizaciones. Es por esto que es recomendable agrupar los activos de acuerdo al nivel de criticidad para la organización y de esta forma evaluar frente a cada uno los riesgos expuestos anteriormente si es conveniente para la organización llevarlos a la nube.

6.2.3 Criterios de evaluación para selección del proveedor de la nube. Para seleccionar el proveedor en la nube se deben tener en cuenta los siguientes aspectos como: ¿Quién accede a los datos?, ¿Quién los puede ver?, ¿Qué es lo que hacen con ellos? ¿Dónde están los datos?, O si se diera un incidente ¿Quién es el responsable, cómo localizarlo o cómo hacerlo responsable de sus actos?

Las respuestas a los anteriores interrogantes permiten establecer el CSP con el cual la entidad debe adquirir el servicio. Aspectos como la protección de los datos, la seguridad en el almacenamiento de los datos en reposo o en tránsito, el acceso de las autoridades policiales, la preservación de la confidencialidad y no divulgación, deben estar estipulados en los contratos y deben ser considerados dentro de los SLA (Acuerdos de nivel de servicio) del mismo.

De acuerdo al análisis planteado por las diferentes entidades anteriormente expuestas, a continuación se describen los aspectos más relevantes que se

considera debe cumplir el CSP y deben ser estipulados en un contrato con un proveedor de servicios en la nube.

- Control de acceso. Por lo general, la mayoría de las infraestructuras son compartidas por múltiples empresas, por esto se debe definir controles de acceso rigurosos, para evitar accesos no autorizados a datos confidenciales. La definición de una buena política de autenticación y control de acceso basada en políticas de mínimo privilegio es fundamental en estos ambientes. El CSP debe garantizar dicha autenticación, autorización con un método de autenticación fuerte de dos factores, acordes a la organización.

- Se debe tener especial atención que el proveedor de servicios en la nube contratado cumpla con las normativas vigentes en Colombia para la protección de datos personales (ley 1581 art 15), Decreto 1377 de 2013 la cual reglamenta la transmisión internacional de datos personales y demás normativas estipuladas en el numeral 6.2 del presente capítulo, dado que estas infraestructuras pueden gestionar los datos en múltiples países lo que puede generar conflictos en cuanto al marco legal en el que son tratados.

- Supervisión de las listas negras públicas para los bloques de red propios.

- Exigir transparencia de la seguridad de la información, el proveedor debe presentar el plan de seguridad, prácticas de gestión, así como informes periódicos de sus cumplimientos. Lo anterior involucra auditorías, pruebas de vulnerabilidad, las medidas que contrarresten, eliminen o traten los hallazgos y hardening de la infraestructura que hace parte del servicio.

- Se deben estipular los mecanismos de notificación ante una violación de seguridad y los métodos empleados de detección y atención por parte de CSP.

- Se debe determinar en el contrato los modelos utilizados de desinfección de software malicioso como acciones preventivas, e informar los hallazgos realizados por la aplicación de este proceso.

- Se debe especificar en el contrato el tipo de cifrado, y la forma en que se protegerá la integridad de los datos en reposo y en tránsito.

- El proveedor deberá contar con procedimientos de generación, almacenamiento y administración de claves fuertes.

- Contractualmente se debe especificar el método de monitoreo de la infraestructura, de la seguridad física y lógica de los componentes de forma proactiva, para de esta forma detectar cualquier actividad no autorizada.

- El proveedor debe suministrar la arquitectura que hace parte del servicio (virtualización, redes, seguridad perimetral, tecnologías de aislamiento...), así como la ubicación de los servicios contratados. Si en dado caso durante la vigencia del contrato esta cambiase, debe informar oportunamente a la entidad contratante.

- Se debe estipular en las cláusulas del contrato, los procedimientos del CSP para la gestión de incidentes, la reanudación y recuperación en el momento en que se presente un desastre. Teniendo claramente definido el RPO (Punto Objetivo de Recuperación) y el RTO (Tiempo objetivo de recuperación) de la organización.

- Se debe estipular los procedimientos, responsabilidades y roles del CSP ante un incidente, asegurando de que se conozcan los requerimientos de la organización contratante. Las respuestas a incidentes deben ser documentados y notificados oportunamente durante y después del mismo.

- El CSP debe realizar la Gestión de los Servicios Informáticos basado en una de las metodologías de gestión de procesos reconocidas como ITIL u otras.

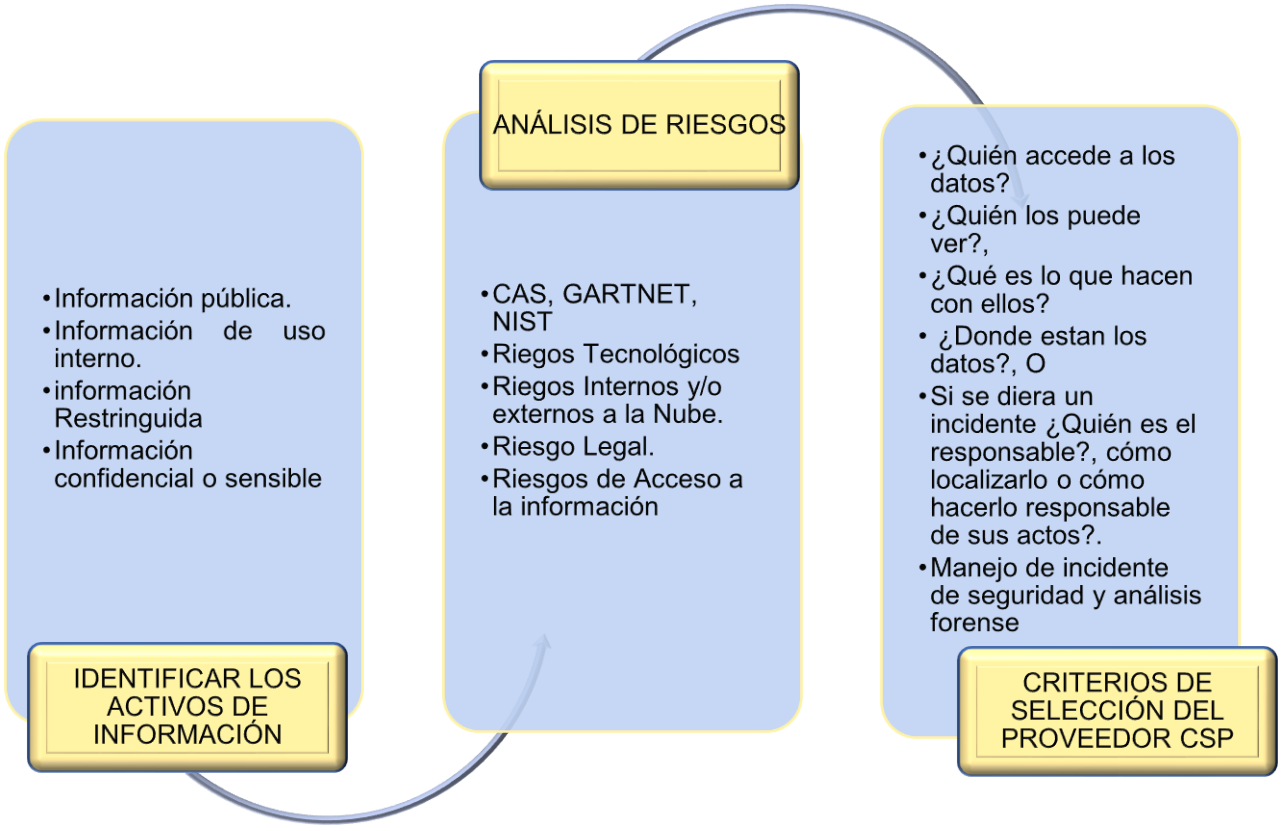
- Se debe estipular en el contrato una cláusula en la cual el CSP, debe contar con personal idóneo y capacitado, con las dimensiones técnicas y herramientas necesarias, para llevar a cabo el proceso forense en entornos en la nube cuando sea requerida por la organización o un ente externo. Esto incluye la recopilación de datos forense, medicina forense elásticas / static / live, segregación de pruebas, investigación en entornos virtualizados etc.

También es necesario contar con acuerdos que habiliten a peritos informáticos solicitar a los proveedores dicha información. Estos acuerdos, idealmente, deberán ser internacionales ya que dado el alcance global de los servicios en la nube.

Todos los puntos expuestos anteriormente deben ser considerados en los contratos de acuerdo de servicio. A su vez todas las recomendaciones en cuanto a este asunto indican que los análisis de riesgos deben ser revisados y analizados específicamente, detallando los controles, las normativas, las medidas de protección, los plazos de ejecución etc.

En la figura 5, son especificados los puntos más relevantes que deben ser considerados en un contrato en relación con los aspectos técnicos.

Figura 5. Recomendaciones en el aspecto Técnicos



Fuente: Elaboración propia.

6.3 ASPECTOS DEL ANÁLISIS FORENSE DE SERVICIOS EN LA NUBE

A continuación, se describen los aspectos más relevantes del análisis forense, para ello se traerá las normas ISO 27037 (ISO, 2012), ISO 27040 (ISO, 2015) e ISO 27042 (ISO, 2015) y DRAF 8006 (NIST 2014). Estas normas y/o estándares constituyen las mejores prácticas de la informática forense, relacionados con las actividades de identificación, recolección, adquisición, preservación, análisis, interpretación y reporte de incidentes; a su vez se expondrán los problemas y desafíos a que se enfrenta las organizaciones cuando es requerido un análisis forense en la nube.

De acuerdo al análisis anterior se dará una serie de recomendaciones que es necesario tener en cuenta en el momento de efectuar un contrato con un proveedor de servicio en la nube.

A continuación, se menciona lo más relevante de dichas normas:

6.3.1 ISO 27037 - Normalizando la Práctica Forense Informática. Es un estándar internacional publicado en el 2012, aplicable internacionalmente, el cual está orientado a proporcionar una guía para una correcta identificación, recolección, recepción, adquisición, manejo, protección y preservación de las pruebas forenses digitales, con el fin de conservar su integridad.

La norma está basada en los siguientes principios:

- Relevancia: lo que quiere decir que la evidencia debe ser pertinente a la situación que se desea investigar las cuales deben conducir a dar solución a la hipótesis que se desea demostrar.

- Confiabilidad: La evidencia recolectada debe ser repetible y auditable por un tercero que utilice la misma metodología de análisis con el fin de llegar a los mismos resultados.

- Suficiencia: la evidencia recolectada y analizada debe ser la necesaria para recabar, asegurar y preservar los elementos probatorios, los cuales serán objeto de análisis por técnicos y sometidos a contradicción de acuerdo al ordenamiento jurídico.

Estos son los factores más importantes que toda evidencia digital debe tener para que esta sea relevante en el momento de una investigación en el caso de un incidente de seguridad y deben constituirse en elemento probatorio para determinar las causas, responsables e impacto.

Aspectos Importantes en la Recolección de Evidencias:

- Se debe tener en cuenta las políticas y normas vigentes de la jurisdicción donde ocurre el incidente.

- Los métodos aplicados para la recolección de evidencia digital deben ser ejecutados por personal idóneo y avalado por las leyes del país la cual lo debe realizar del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.

- Se debe identificar la evidencia física y lógica.

- La recolección de la evidencia y los procedimientos utilizados deben ser documentados y previamente validados por las buenas prácticas profesionales, el cual debe incluir fecha, hora y firma.

- Se debe tener en cuenta la diferencia horaria del sistema y la hora UTC y se debe registrar los dos datos.

- La evidencia digital debe ser preservada para asegurar la integridad de la misma. Se debe garantizar la originalidad, la cadena de custodia para su admisión posterior como medio probatorio. Esto incluye el embalaje y cualquier otro requerimiento legal.

- Los métodos y procedimientos aplicados deben de ser validados previamente, reproducibles, verificables y argumentativos al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

- Se debe tener en cuenta la volatilidad de la evidencia recolectada, se debe iniciar por la más susceptible a volatilidad.

Las tipologías de dispositivos y entornos tratados en la norma son los siguientes:

- Equipos y medios de almacenamiento y dispositivos periféricos.
- Sistemas críticos (alta exigencia de disponibilidad).
- Ordenadores y dispositivos conectados en red.
- Dispositivos móviles.
- Sistema de circuito cerrado de televisión digital.

Las tipologías son sensibles a los cambios tecnológicos y nuevos retos emergentes de la informática forense, lo que necesariamente advierte que las técnicas descritas en el estándar deberán ser revisadas y ajustadas en el tiempo de manera periódica.

6.3.2 ISO 27040 - Almacenamiento seguro[28]. Es un estándar que presenta las mejores prácticas para la protección del almacenamiento y da las bases para auditoría, diseño y revisión de controles de seguridad en el almacenamiento. Así mismo advierte de las brechas de seguridad que afectan el almacenamiento, para establecer una ruta de diseño y aseguramiento de estrategias para guardar la información, que implican controles físicos, técnicos y administrativos.

Este estándar no detalla los aspectos relevantes para la informática forense en términos de recuperación y evidencia digital. Pero si expone principios de diseño de almacenamiento seguro como son la defensa en profundidad (acciones basadas en personas, procesos y tecnología), dominios de seguridad (separación de recursos de acuerdo con su nivel de sensibilidad), diseño de resiliencia (eliminación de puntos únicos de falla y maximización de la disponibilidad) e inicialización segura (secuencia de transición desde el estado “caído” a activo, luego de una falla o reinicio de los medios de almacenamiento)[29].

[28] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Tecnología de la información. Técnicas de seguridad. Seguridad de almacenamiento. 2015 (ISO/IEC 27040)
[29] Ibíd., p.1.

6.3.3 ISO 27042 - Guías para el análisis e interpretación de la evidencia digital. Este estándar provee información sobre cómo adelantar un análisis e interpretación de la evidencia digital potencial en un incidente con el fin de identificar y evaluar aquella que se puede utilizar para ayudar a su comprensión. Así mismo, provee un marco común para el análisis e interpretación de la gestión de incidentes de seguridad en sistemas de información, que puede ser utilizado para la implementación de nuevos métodos y proporcionar un estándar mínimo y común para la evidencia digital que se produce a partir de dichas actividades.

El estándar también incluye definiciones importantes para el ejercicio de la informática forense, desde la práctica de ISO. Como, por ejemplo:

Evidencia digital potencial: Información o datos, almacenados o transmitidos en formato binario que no han sido determinados a través un proceso de análisis que sea relevante para la investigación.

Evidencia digital: Información o datos, almacenados o transmitidos en formato binario que han sido determinados a través un proceso de análisis que sea relevante para la investigación.

Evidencia digital legal: Es la evidencia digital que ha sido aceptada en un proceso judicial. (En términos jurídicos es lo que se llama prueba).

Investigación: Aplicación de exámenes, análisis e interpretaciones para entender un incidente.

Examen: Conjunto de procesos aplicados para identificar y recuperar evidencia digital potencial relevante de uno o más fuentes.

Análisis: Evaluación de la evidencia digital potencial con el fin de valorar su relevancia para una investigación, así como los significados de los artefactos digitales latentes en su forma nativa.

Interpretación: Síntesis de una explicación, dentro de los límites acordados, para los hechos revisados acerca de la evidencia resultante de un conjunto de exámenes y análisis que componen la investigación.

El estándar también habla sobre los modelos analíticos que pueden ser usados por los analistas forenses en informática, sobre sistemas estáticos o en vivo.

El análisis estático, es un examen de evidencia digital potencial, por inspección exclusivamente, con el fin de determinar su valor como evidencia digital.

El análisis en vivo, es un examen de evidencia digital potencial en sistemas en vivo o activos. Particularmente útil en sistemas de mensajería instantánea, teléfonos inteligentes/tabletas, intrusiones en redes, redes complejas, dispositivos de almacenamiento cifrado o código polimórfico sospechoso.

Existen dos formas de adelantar el análisis en vivo:

- Análisis en vivo de sistemas que no pueden ser copiados o no se puede capturar la imagen.

- Análisis en vivo de sistemas que pueden ser copiados o se puede capturar la imagen.

En la norma se detalla lo que debe contener el reporte resultado de la pericia adelantada, siempre y cuando no exista alguna indicación jurídica o legal previamente expuesta sobre este tipo de investigaciones realizadas. Las recomendaciones ofrecidas indican que el informe debe contener como mínimo[30]:

- Calificaciones de autor o las competencias para participar en la investigación y producir el informe.

- La información provista al equipo de investigación antes de iniciar la investigación (naturaleza de la información que se va a desarrollar.

- La naturaleza de los incidentes bajo investigación.

- Tiempo y duración del incidente.

- Ubicación del incidente.

- Objetivo de la investigación.

- Miembros del equipo de investigación, sus roles y actuaciones.

[30] Ibíd., p.1.

- Tiempo y duración de la investigación.

- Localización de la investigación.

- Hechos concretos soportados por evidencia digital hallados durante la investigación.

- Cualquier daño a la evidencia digital potencial que se pueda haber observado durante la investigación y sus impactos en los siguientes pasos del proceso.

- Limitaciones de cualquiera de los análisis realizados.

- Listado de procesos utilizados, incluyendo donde sea apropiado, cualquier herramienta usada.

- Interpretación de la evidencia digital por parte de investigador.

- Conclusiones.

- Recomendaciones para futuras investigaciones o acciones de remediación.

Finalmente se insiste, en que las opiniones del investigador se deben separar claramente de los hechos. Las opiniones deben ser debidamente justificadas y asistidas de la formalidad científica que le corresponde y no deben estar asociadas con juicios de valor mal fundados o impresiones de sus análisis.

El estándar ISO 27042, concluye con algunas indicaciones sobre la competencia de los analistas forenses, entendidas como un “saber hacer” especializado, las cuales hablan sobre la formación, mantenimiento y aseguramiento de las habilidades requeridas para ejecutar las actividades propias de la gestión de la evidencia digital.

El dominio o pericia comprobada, se debe validar por parte de terceros independientes. De no poderse hacer, se deberá consultar equipos de investigación para establecer esquemas de validación para sus propias necesidades. Estos esquemas deben ser sometidos a revisión independiente, para verificar si son apropiados.

El análisis de dichas normas fue tomado del documento referenciado en la nota de pie de página[31].

6.3.4 Norma DRAFt 8006 NIST 2014. Esta norma es producto del trabajo de investigación desarrollado por miembro de la NIST orientado al estudio de los desafíos a que se enfrenta la ciencia forense, en respuesta de un incidente de seguridad que se presente en la nube. Así mismo, el objetivo de este grupo es identificar tecnologías y estándares que puedan ser implementados para dar solución a los problemas a que se enfrenta el análisis forense en la nube.

La idoneidad de la ciencia forense en un ambiente en la nube busca extraer la finalidad de la ciencia aplicada en un ambiente tradicional, pero de acuerdo como se describe en el documento, el enfoque en un ambiente en la nube requiere de nuevas metodologías para identificar, recopilar, conservar y analizar evidencia, por las características especiales en la nube de compartir una misma infraestructura por múltiples organizaciones y por el acceso a la misma.

De acuerdo a la norma, la ciencia forense de computación en la nube se define como: “Aplicación de principios científicos, practicas, tecnologías y métodos derivados y probados para reconstruir eventos sados de computación en la nube, mediante la identificación, recolección, preservación, examen e interpretación de pruebas digitales” [32] .

El desarrollo de este trabajo implica que se analicen e involucren diversos componentes y aspectos que hacen parte de la infraestructura en la nube (los cuales no hacen parte de una infraestructura tradicional), entre los cuales se encuentran el enfoque virtual de red a gran escala, cliente liviano y pesado etc., de igual forma los diferentes actores que hacen parte de un servicio en la nube, los cuales fueron explicados en el numeral 5.1.3 (proveedor, el consumidor de la nube, el corredor, operador y auditor). A su vez se deben evaluar aspectos de multi-jurisdicción y servicios compartidos con otros usuarios y organizaciones.

La presente norma respeta y sigue los procedimientos de recolección y análisis de evidencias descritos en el numeral 6.3.1 y 6.3.3 de este documento, pero se

[31] IT-INSECURITY. 2015. La investigación forense informática. Tensiones emergentes entre los estándares vigentes y el ecosistema digital. *IT-Insecurity.* [En línea]. < http://insecurityit.blogspot.com.co/2015/06/la-investigacion-forense-informatica.html> [citado en 28 de Junio de 2015].
[32] NIST. 2014. NIST Cloud Computing Forensic Science Challenges . *Naional Institute of Standards and Technology.* [En línea]. <http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf> [citado en Junio de 2014].

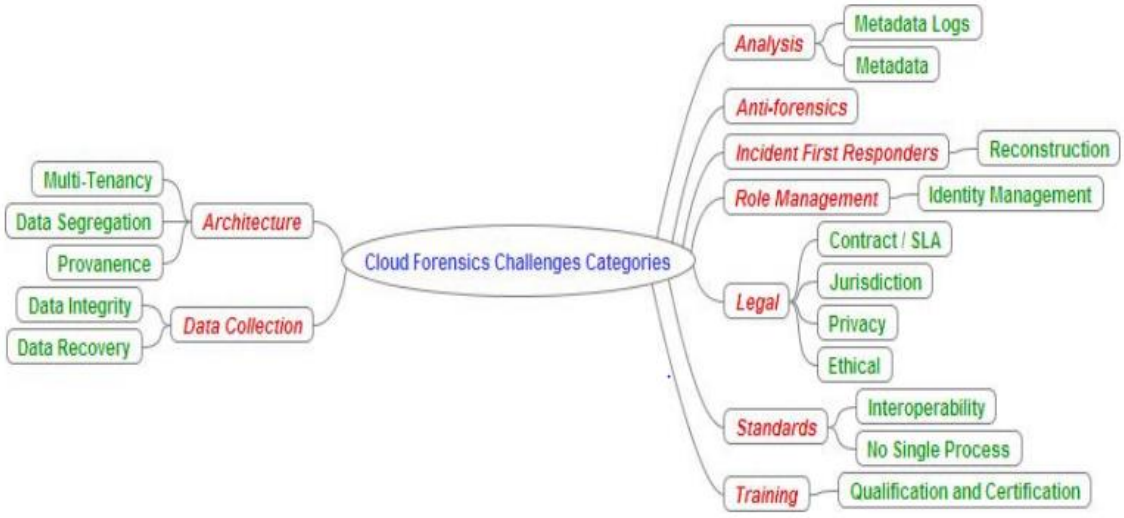
destaca nuevos desafíos inherente de la nube, los cuales deberán ser atendidos desde la óptica tecnológica, legal y organizacional en conjunto.

Entre estos desafíos encontramos:

- Segregación de tareas entre los actores de la nube.
- Dificultad de adquirir registro de red de equipos de carga y/o routers.
- Retos asociados a la virtualización de datos a gran escala.
- Procesamiento y la proliferación de dispositivos móviles.

Dentro de este trabajo los desafíos fueron clasificados en nueve categorías las cuales se pueden evidenciar en la Figura 6 y se describen con más detalle a continuación:

Figura 6. Desafíos de ciencia forense en la nube, Categorías y subcategorías



Fuente: NIST, 2014.

6.3.4.1 Categorías. Los desafíos evidenciados se agruparon en nueve categorías las cuales se describen a continuación:

- Arquitectura. El reto de la ciencia forense en la nube, implica el reconocimiento de diversidad de arquitecturas de los diferentes proveedores, entre los que se encuentra enfrentarse con plataformas compartidas, aislamiento durante el aprovisionamiento de recursos, ubicación y puntos finales donde se pueden guardar datos.

- Recolección de datos. Se refiere a la integridad de datos, recuperación, localización de datos e imágenes los cuales se encuentran distribuidos y bajos sistemas dinámicos. Recolección de datos volátiles, recuperación de datos borrados y máquinas virtuales, en un ambiente compartido en el que se debe respetar la confidencialidad de la información de otros que hacen uso y comparten la infraestructura.

- Análisis. Incluye la correlación de artefacto forenses a través y dentro de los proveedores de servicios, reconstrucción de eventos a partir de imágenes virtuales, e integridad de los metadatos, análisis de la línea del tiempo y log de datos.

- Anti-forense. Es el conjunto de técnicas desarrolladas especialmente para prevenir el análisis forense. El mayor desafío del análisis forense en la nube debe incluir la ofuscación, malware, ocultación de datos y otros aspectos que alteren la integridad de la evidencia.

- Primer Respondiente. Confiabilidad en la competencia y fiabilidad de los proveedores y actores para actuar como primera respuesta a un incidente para tratar temas de recolección de datos y el manejo de las diferentes herramientas forenses.

- Gestión de funciones. Por ejemplo, propiedad de los datos, gestión de identidades, usuarios, control de accesos. Este reto en el área forense en la nube incluye la identificación exclusiva de cada cuenta de acceso, desacoplamiento de las credenciales de usuarios de la nube y usuarios físicos, lo que puede ayudar a determinar la propiedad de los datos, autenticación y control de acceso.

- Legal. Los desafíos en el área legal incluyen abordar aspectos de jurisdicción para el acceso a los datos. Falta de acuerdos entre proveedores efectivos de cooperación durante la investigación, en cuanto a se refiere a la recolección de datos su competencia y fiabilidad, los cuales deben ser especificados con claridad en los ANS. Desconocimiento de la ubicación física de los datos y proferir incautación puede interferir con la continuidad del servicio de otros usuarios del servicio.

- Estándares. Este desafío se refiere a la falta de interoperabilidad de los proveedores de la nube, ausencia de estándares de operación y herramientas de validación de procedimientos.

- Capacitación: Se refiere al mal uso de prácticas forenses que no son aplicables en servicios en la nube. La falta de formación y experiencia forense en la nube

6.4 ANÁLISIS

En una arquitectura tradicional de computación los investigadores forenses tienen el control de cada uno de los componentes que hacen parte de una escena forense (discos duros, videos, equipos de comunicaciones, pc, etc.), por el contrario, en un ambiente en la nube se encuentran estos componentes de forma distribuida y por lo tanto el control varía entre los actores de la nube de acuerdo al modelo de servicio. No en todos se tiene el mismo control, por ejemplo, es mayor el control en un nivel de IaaS que en la que se pueda tener en un Saas y por lo mismo los métodos que se apliquen para la recolección de evidencias varían.

De igual forma se deben considerar todas las posibles fuentes de análisis forense, unas más fáciles de acceder que otras debido a la estructura de las mismas, lo anterior debido a la separación de tareas entre los diferentes actores y factores de integridad de los mismos. Tres ejemplos de estas fuentes son auditoría, seguridad y registros de aplicaciones.

Los registros de auditoría son los registros de las interacciones entre los servicios. Los registros de seguridad rastrean los usuarios y sus acciones, identificando el usuario en particular que tomó una acción y la fecha de ocurrencia. Por último y no menos importante los registros de aplicación, los cuales almacenan la actividad generada por las aplicaciones con errores y otras fallas operacionales de estas.

Por otra parte, la identificación, recolección y preservación de evidencia y de los medios de comunicación puede ser particularmente difícil, para esto se debe considerar:

- Identificar el proveedor y sus terceros, necesario para tener un mejor entendimiento de la infraestructura, su topología, políticas y actores que componen el servicio contratado.

- La capacidad de identificar de manera concluyente las cuentas apropiadas mantenidas dentro de la nube por un consumidor.

- La capacidad del especialista y una vez obtenido el acceso, la capacidad del examinador para completar una imagen forense de los medios de comunicación.

- El volumen de los medios de comunicación y de la información.

- La capacidad de responder oportunamente a más de un lugar físico si es necesario.

- Recopilación de archivos de registro respetando los derechos de privacidad dados de otros usuarios o clientes de la nube. ¿Cómo recoger registros pertinentes a la investigación sin ir en contra de la protección de los derechos de privacidad?

- Validación de la imagen forense, con métodos avalados por la jurisprudencia competente.

- La capacidad de realizar análisis en datos cifrados.

- El sistema de almacenamiento ya no es local.

- A menudo no hay forma de vincular pruebas dadas a un sospechoso en particular, confianza en el proveedor.

Los anteriores aspectos deben atender adecuadamente las necesidades del primer respondiente y los sistemas judiciales, al mismo tiempo asegurar a los proveedores de la nube que este proceso no generara ninguna interrupción o una interrupción mínima del servicio.

Otro aspecto que deberá asegurar es llegar a efectuar la recolección legítima de pruebas forenses digitales de manera remota ya que reducirán los costos de viajes. En esencia, esto implicará mover imágenes forenses electrónicamente desde el proveedor de la nube a un laboratorio forense. Mejor aún, sería realizar el forense de una manera científica en la nube

Se requiere más investigación en el dominio de la nube que permita identificar y clasificar los aspectos de dónde y cómo se puede encontrar la evidencia digital, ya que resulta dispendioso y complejo llegar a puntos usuarios finales, como los dispositivos móviles. La evidencia digital se puede encontrar en las que incluye numerosas computadoras, así como dispositivos periféricos etc.

Teniendo en cuenta estos estándares es necesario tener en cuenta las siguientes recomendaciones para garantizar un excelente proceso en el análisis forense ante la aparición de un incidente de seguridad que afecte la prestación del servicio contratado o que comprometa la información almacenada en la nube.

6.4.1 Establecer legalmente la obligación del proveedor del servicio en la nube a brindar la información solicitada. Entendiendo el objetivo de la informática forense y teniendo en cuenta las características de computación en la nube, se hace difícil la actividad de análisis forense en la nube sin colaboración del cada uno de los actores del servicio y de expertos forenses en la nube, para la identificación, adquisición y análisis de los datos.

6.4.2 Delegar la tarea de recolección al proveedor del servicio en la nube. Con los servicios en la nube surge el problema de la imposibilidad de acceder a los medios físicos donde se encuentra ubicada la información debido a:

- La subcontratación de servicios: puede que el proveedor del servicio sea a su vez cliente de otro servicio de nube, y no disponga de servidor propio. Por esta razón el proveedor puede no conocer la ubicación física de los datos y habría que recurrir al proveedor de segundo nivel (el proveedor del proveedor).

- Locación distribuida: los datos del sistema del servicio tienen locación distribuida, es decir que la información no se encuentre en un único servidor físico.

- Recursos compartidos: los recursos de los servicios de nube son compartidos por varios clientes, los cuales son ajenos a la investigación con derechos sobre

su información y el uso del sistema. Por lo tanto, es posible que no se puedan retener dichos recursos como evidencia, y las copias de información deban realizarse con el sistema en funcionamiento.

Por estos motivos, se recomienda delegar la tarea de recolección al proveedor del sistema, y que disponga de los medios para obtener y aislar los datos que serán presentados al equipo forense.

6.4.3 Extraer como evidencia solo lo relacionado al cliente de la investigación. Muchos clientes del servicio pueden tener su información en la misma locación (física o virtual). En el proceso de una investigación esa información debe ser protegida y extraer como evidencia solo lo relacionado al cliente de la investigación. Esto es una tarea que debe realizar el proveedor del servicio; ya que, aun teniendo acceso directo a los recursos, por parte de un investigador, es complicado discriminar cuáles datos corresponden a cada cliente.

6.4.4 El proveedor del servicio y los diferentes actores deben brindar la documentación necesaria para la correcta interpretación de los datos adquiridos. Es evidente que la participación y la dependencia del proveedor y los actores del servicio son decisivos para el desarrollo de una investigación. De no contar con el apoyo del proveedor; adquirir, obtener y preservar los datos sería una tarea muy difícil. Por ello es necesario contar con acuerdos que faciliten a los investigadores informáticos los medios para solicitar a los proveedores dicha información. Estos acuerdos, deberían ser internacionales debido al alcance global de los servicios de computación en la nube.

La dependencia de los proveedores de servicios, no es un problema solamente a nivel técnico, sino también legal. Pero conociendo los entornos, en los aspectos legales y técnicos, los problemas de computación en la nube tienen solución.

En la Figura 7 se pueden ver claramente las recomendaciones en el aspecto forense.

Figura 7. Recomendaciones para el Análisis Forense

Fuente: Elaboración propia.

6.5 GUÍA DE CONTRATACIÓN

De acuerdo con el estudio y la investigación realizada durante el desarrollo de presente trabajo en la tabla 4 se puntualizan los aspectos desarrollados en esta guía y que se deben tener en cuenta en la celebración de un contrato de servicios en la nube con un proveedor de este servicio y que garantice un correcto análisis forense cuando se presente un incidente de seguridad.

En primera instancia, dentro del contrato se debe establecer un Anexo que especifique el acuerdo de servicio con relación a la atención de incidentes de seguridad, en el cual se deben registrar los factores a los que se comprometen cada una de las partes para el desarrollo de un análisis forense en la nube en el momento de requerirse.

Tabla 4. Guía de Contratación

ASPECTOS	RECOMENDACIONES
Jurídicos	– Definir las condiciones de la relación jurídica y la legislación aplicable al contrato, siendo puntual en estipular aspectos de confidencialidad de datos personales y transferencia internacional de datos; el proveedor y los diferentes actores deben garantizar niveles adecuados de seguridad (ley 1581.2012). – Definir el lugar donde estará alojada la información. En caso de que se realice una migración a otro centro de datos o país por cualquier motivo atribuible al proveedor, se debe garantizar que será informado y se deben respetar los acuerdos establecidos a nivel de políticas de tratamiento de datos personales y legislación mencionados anteriormente – Realizar el ejercicio de derecho comparado. Teniendo claro las leyes vigentes del estado colombiano en relación al manejo de datos personales, privacidad y transferencia de datos personales, así mismo conocer las leyes vigentes en el (os) país (es) donde estará alojada la información, las cuales deben tener similitud con las de Colombia. – Determinar la distribución de responsabilidades entre los que intervienen en la provisión del servicio al momento en que se requiera realizar una investigación forense. Teniendo en cuenta que en un servicio puede haber un proveedor de la infraestructura física, otro que disponga de los servidores que brinden espacio de almacenamiento y tiempo de procesamiento, otro que monte una plataforma de software como servicio, etc. por esta razón se debe determinar el nivel de participación de cada proveedor. – Definir el alcance jurisdiccional del contrato. Para ello se deben establecer en el contrato acuerdos de cooperación durante la investigación en que el proveedor y los terceros se comprometan en cuanto a la recolección de datos, a su competencia y fiabilidad, los cuales deben ser especificados con claridad en los ANS.

Tabla 4. (Continuación)

ASPECTOS	RECOMENDACIONES
Técnicos	– Se debe estipular en el contrato los componentes de la arquitectura del servicio y actores de servicio. Así mismo se debe definir que si durante la vigencia del contrato alguno de estos es cambiado o modificado por mejoras o incidentes presentados, o por cambio de terceros o de ubicación de los datos, debe ser comunicado con antelación al contratante, para que de esta forma se de una trazabilidad del servicio por las partes involucradas y en el momento de un incidente que se refiera a un análisis forense, se tenga clara la ubicación y los componentes involucrados en la investigación. – Establecer la propiedad de los datos. – Distribución de responsabilidades ante un incidente de seguridad y tiempo de respuesta ante una investigación forense. Para ello se deben establecer ANS de cumplimiento dentro de contrato. – Manejo de incidentes. Establecer los ANS relativos a la atención de los incidentes de acuerdo a su nivel de impacto. Se debe dar a conocer a la organización contratante la metodología que emplea el proveedor y los actores del servicio para enfrentar un incidente, el control y seguimiento a esta metodología, monitoreo, planes de emergencia, atención, contención y erradicación. Debe quedar definido en el contrato la entrega de informes periódicos de los incidentes presentados, estadísticas, acciones de mejora y de igual forma cuántos de ellos afectaron el servicio contratado. También se deben definir los ANS relativos a la atención de los incidentes conforme a su nivel de impacto. – Debe quedar establecido en el contrato que el proveedor y sus terceros deben evaluar la plataforma de seguridad, garantizando el análisis de vulnerabilidades por lo menos dos veces al año, mecanismos de hardening y re-test. Producto de esto realizara entregas sobre los resultados de estas actividades.

Tabla 4. (Continuación)

ASPECTOS	RECOMENDACIONES
	– ¿Quién accede a los datos? Para ello se debe establecer en el contrato los mecanismos utilizados por los funcionarios del proveedor y sus actores a la infraestructura y la información alojada en ella. Seguridad de contraseñas fuertes (doble factor) y control de acceso. Así mismo, se deben separar los mecanismos de autenticación y credenciales de acceso empleadas por usuarios de la nube a la de usuarios físicos o funcionarios que interactúan con la plataforma. – Se debe informar al proveedor en el momento de la firma del contrato cual es la información que se considerada como sensible para que tenga un manejo diferente, para el caso de un incidente que requiera análisis forense, se de una oportuna respuesta teniendo en cuenta la importancia para la organización. – En el contrato debe quedar estipulado el compromiso del proveedor de servicios en la nube en relación al manejo de la información de bases de datos, servidores, licencias y otras. El incumplimiento de la misma podrá ser causa de acciones civiles y penales aplicables al derecho internacional sobre este aspecto.
Forenses	– Definir que se permita el acceso a todas las fuentes de análisis forense entre ellas están log, registros de auditorías, registros de seguridad (rastreo de usuarios y acciones), y registros de aplicaciones (errores y fallas operacionales). – Establecer si el proveedor realizar el análisis forense y/o si permite ingresar a un especialista para la reconstrucción del evento y recolección de imágenes virtuales, datos volátiles, metadatos, etc. Si se da el primer caso se debe solicitar en el contrato que el proveedor debe contar con peritos forenses especializados, los cuales deben tener certificaciones internacionales avaladas por las leyes colombianas en esta práctica.

Tabla 4. (Continuación)

ASPECTOS	RECOMENDACIONES
Forenses	Se debe considerar en este punto que el análisis forense que se requiere estará en la nube, por lo anterior los especialistas deben contar con experiencia en este ambiente. – Se puede definir, en algunas ocasiones, de acuerdo al impacto del incidente, si este análisis forense se puede realizar en forma remota, mediante ejecutables desarrollados para tal fin, y establecer los mecanismos de confiabilidad e integridad de las evidencias recolectadas las cuales serán entregadas por parte del operador y los actores del servicio. – Estipular en el contrato la responsabilidad del proveedor del servicio y sus actores de garantizar que la información vinculante que se encuentre en la nube, no se verá afectada durante un proceso de análisis forense, para ello será el quien determine los procedimientos y metodologías que se emplearan para separar la información vinculante a una investigación forense, sin que ello afecte la confiabilidad e integridad de la recolección y custodia de la evidencia que se requiera y a su vez viole la privacidad de la información de otros usuarios de la plataforma. – Existen algunos componentes a los cuales es difícil llegar y por lo cual no es posible realizar análisis forense en evento que se requiera, estos son los dispositivos finales a través de los cuales son accedidos los recursos de la nube y que no están definidos su ubicación y los cuales no están bajo el dominio de los actores del servicio, es por esto que es necesario que el proveedor tenga un buen procedimiento de control de acceso y seguridad de autenticación y defensa en profundidad.

Fuente: Elaboración propia.

Es importante tener en cuenta que las anteriores recomendaciones de la guía van de acuerdo al tipo de organización contratante y del servicio contratado y no son vinculantes en todo contrato de servicios en la nube.

7. CONCLUSIONES

En el logro de la investigación realizada se puede evidenciar el conocimiento adquirido en los aspectos legales vigentes frente a la contratación de servicios en la nube, así como los aspectos técnicos y forenses que dan como resultado una guía para la contratación de servicios en la nube que garanticen un correcto análisis forense cuando se presente un incidente de seguridad.

El haber realizado el estudio de los estándares dados por la ISO, la NIST y otros estudios elaborados por organizaciones de tecnología y computación en el tema, y analizando cada uno de los desafíos que se encuentran en la nube frente a seguridad y análisis forense, se entrega como resultado una serie de recomendaciones que facilitan a las empresas Colombianas realizar un contrato que garantice una respuesta adecuada para el análisis forense al momento en que se presente un incidente de seguridad. Una mala definición de los acuerdos en el contrato puede conllevar a la imposibilidad en un futuro, de encontrar la evidencia digital necesaria, para dilucidar responsabilidades, y en consecuencia acarrear perjuicios para la organización de índole económica, civil y penal.

8. RECOMENDACIONES

Una organización antes de seleccionar un CSP y de la firma del contrato, debe realizar un análisis de riesgos de cada uno de los principales activos de información, como responsable de la misma, y de esta forma determinar cuál de ellos llevar a la nube (privada, pública, hibrida o comunitaria). Para este ejercicio se debe tener en cuenta el impacto implícito frente a los riesgos de la nube; más aún, ahondar cual es el impacto que esto sugiere en caso de requerirse una evidencia digital (económico, prestigio, jurídico). “Mientras mejor conozcamos donde se puede albergar aquella evidencia digital derivada de un incidente en “la nube”, mayor seguridad tendrá la organización para depurar responsabilidad ante un proceso judicial”. [33]

Si bien en la actualidad no existen estándares, leyes y/o normas nacionales ni internacionales en las cuales se pueda amparar o sustentar un análisis forense en la nube, ya que la literatura existente soporta esta práctica en los ambientes tradicionales, los desafíos que implica esta actividad en la nube puede considerarse como buen punto de partida para tener en cuenta en el momento de firmar un contrato con un CSP. Por esta razón es necesario aplicar cada una de las recomendaciones dadas en este guía para garantizar una adecuada contratación de servicios en la nube, teniendo en cuenta los aspectos necesarios para realizar un análisis forense en caso que se presente un incidente de seguridad.

[33] LLEIXÀ I ALSINA, Ángela. 2015. La evidencia digital ante riesgos y amenazas en el Cloud Computing. Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. [En línea]. <http://www.aspectosprofesionales.info/2015/06/la-evidencia-digital-ante-riesgos-y.html> [citado en 6 de Junio de 2015].

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. S.F Glosario de términos. [En línea]. https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php

AREOS, Israel. 2015. Artefactos Forenses I. [En línea]. http://insecuredata.blogspot.com.co/2015/03/artefactos-forenses-i.html [citado en 17 de Marzo de 2015].

BOHN, Robert y TOBIAS, James. Cloud Computing and Accessibility Considerations. National Institute of Standards and Technology. [En línea]. https://www.nist.gov/sites/default/files/documents/itl/cloud/sp500-317_v01-draft.pdf [citado en Marzo de 2016].

BOHN, Robert. Cloud Computing Standards – A NIST Perspective. Cloud Standards Coordination – ETSI . [En línea]. < http://csc.etsi.org/resources/2016-0128-Final-Presentation/Speakers---NIST---BBohn.pdf> [citado en 28 de Enero de 2016].

CUIDA TUS DATOS. S.f. ¿Qué es un tratamiento de datos personales? [En línea]. <http://www.cuidatusdatos.com/infotratamiento.html>.

ENCICLOPEDIA JURÍDICA. S.f. Derecho comparado. Enciclopedia jurídica. [En línea]. <http://www.enciclopedia-juridica.biz14.com/d/derecho-comparado/derecho-comparado.htm> [citado en S.f].

GARCÍA, Esteban, Roberto. Cloud a cuatro años vista: el futuro de la nube. A un clic de las TIC. [En línea]. <http://aunclicdelastic.blogthinkbig.com/cloud-2020-el-futuro-de-la-nube/> [citado en 10 de Mayo de 2016].

GARTNER. S.f. Gartner. [En línea]. <http://www.gartner.com/technology/why_gartner.jsp>.

GESTIÓN CALIDAD. 2016. Definiciones: Seguridad de la Información SI: Activos. [En línea]. <http://gestion-calidad.com/definiciones-seguridad-informacion [citado en 7 de Septiembre de 2016].

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. 2006. Tecnología de la información. Técnicas de seguridad. Sitemas de gestión de la seguridad de la información (SGSA). Requisitos. Bogotá: ICONTEC, 2006 (NTC-ISO/IEC 27001).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Tecnología de la información. Técnicas de seguridad. Seguridad de almacenamiento. 2015 (ISO/IEC 27040)

IT-INSECURITY. 2015. La investigación forense informática. Tensiones emergentes entre los estándares vigentes y el ecosistema digital. IT-Insecurity. [En línea]. < http://insecurityit.blogspot.com.co/2015/06/la-investigacion-forense-informatica.html> [citado en 28 de Junio de 2015].

ITU-T. 2014. Series y: Global information infraestructure, internet protocol aspects and next-generation networks. International Telecomunication Union. [En línea]. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3502-201408-I!!PDF-E&type=items [citado en Agosto de 2014].

LEÓN VELANDIA, Beimar. 2014. Metodología y recomendaciones para la contratación de servicios en la nube para empresas estatales en Colombia. Bogotá D.C, 2014, 156 h. Tesis de investigación (Magister en Ingeniería-Telecomunicaciones). Universidad Nacional de Colombia. Facultad de Ingeniería. Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial. Disponible en el catálogo en línea de la Biblioteca de la Universidad Nacional de Colombia:<http://www.bdigital.unal.edu.co/46259/1/2707129.2014.pdf>.

LIU, Fang, et al. 2011. NIST Cloud Computing Reference Architecture. National Institute of Standards and Technology. [En línea]. <http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505> [citado en Septiembre de 2011].

LLEIXÀ I ALSINA, Ángela. 2015. La evidencia digital ante riesgos y amenazas en el Cloud Computing. Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. [En línea].

<http://www.aspectosprofesionales.info/2015/06/la-evidencia-digital-ante-riesgos-y.html> [citado en 6 de Junio de 2015].

MARTÍN, Eduardo. 2014. ¿Qué es 'cloud computing'? Definición y concepto para neófitos. TICbeat. [En línea]. <http://www.ticbeat.com/cloud/que-es-cloud-computing-definicion-concepto-para-neofito> [citado en 2 de Diciembre de 2014].

MELL, Peter y GRANCE, Timithy. 2014. The NIST Definition of Cloud Computing. National Institute of Standards and Technology. [En línea] <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [citado en 2014].

NIST. 2014. NIST Cloud Computing Forensic Science Challenges . Naional Institute of Standards and Technology. [En línea]. <http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf> [citado en Junio de 2014].

NORMA CHILENA. 2013. Tecnología de la información. Técnicas de la seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. 25 de Octubre de 2013. (NCh-ISO 27001).

PÉREZ, Julián y GARDEY, Ana. 2012. Definición de Ofuscación. [En línea]. http://definicion.de/ofuscacion/.

RIVERO, Marcelo. S.f. ¿Qué son los Malwares? [En línea]. https://www.infospyware.com/articulos/que-son-los-malwares/.

SEARCH DATA CENTER. 2012. Equipo de Respuesta frente a incidentes de seguridad informática (CSIRT). [En línea]. <http://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT> [citado en Noviembre de 2012].

SLA. S.f. Acuerdo de Nivel de Servicio. [En línea]. http://asi-ut.bligoo.com.co/media/users/31/1555916/files/563120/Adsi_T3_Acuerdo_de_Nivel_de_Servicio_SLA.pdf

VELASCO & CALLE D´ALEMAN. 2016. Contratación en la Nube, Privacidad y recomendaciones de la Autoridad colombiana. (Parte 1). Velasco & Calle

D´Aleman. [En línea]. <http://velascocalle.co/blog/contratacion-en-la-nube-privacidad-y-recomendaciones-de-la-autoridad-colombiana-parte-1/> [citado en 12 de Julio de 2016].

GUÍA DE CONTRATACIÓN DE SERVICIOS EN LA NUBE PARA EMPRESAS PÚBLICAS Y PRIVADAS EN COLOMBIA QUE GARANTICE UN CORRECTO ANÁLISIS FORENSE CUANDO SE PRESENTEN INCIDENTES DE SEGURIDAD

Martha Carolina Preciado Becerra
e-mail: mprecibe@banrep.gov.co
Magda Luz Vargas Herrera
e-mail: magluz30@gmail.com

RESUMEN: *El presente trabajo busca desarrollar una guía, soportada por las leyes vigentes en Colombia, que le permitan a las empresas públicas y privadas realizar un contrato de servicios en la nube con empresas nacionales o internacionales, en el cual se contemplen los aspectos principales que amparen a la entidad y exijan al CSP llevar a cabo un correcto análisis forense en caso de que un incidente de seguridad lo requiera.*

PALABRAS CLAVE: *Guía, Servicios en la nube, análisis forense, incidentes de seguridad, Colombia*

ABSTRACT:
The present work seeks to develop a guide, supported by the laws in force in Colombia, that allow public and private companies to enter into a contract for services in the cloud with national or international companies, in which the main aspects that cover the entity and require the CSP to carry out a correct forensic analysis in the event that a security incident requires it..

KEYWORDS: *Guide, Cloud Services, Forensic Analysis, Security Incidents, Colombia*

1. INTRODUCCIÓN

En la actualidad las nuevas tecnologías de la información proporcionan a las entidades y/o personas la posibilidad de migrar a plataformas que suministren una mayor disponibilidad, eficiencia e inmediatez de la información a bajos costos. Ante este panorama surgen tecnologías como "Cloud computing o información en la nube", que brinda características que buscan las empresas hoy en día, donde el manejo y la disposición de la información y aplicaciones es proporcionado por un tercero, sin que la compañía asuma costos de adquisición, administración y manejo de una infraestructura tecnológica que lo soporte.

Aunque los proveedores de servicio en la nube garantizan un alto grado de seguridad para el acceso y control de la información que manejan de sus clientes, aún hay incertidumbre ante cómo enfrentar un incidente que afecte el servicio o la seguridad de la compañía de forma legal y en la que se requiera un análisis forense digital, ¿Cómo será la cadena de custodia de la información?, ¿Qué leyes amparan el procedimiento?, ¿Quienes tendrán la potestad de autorizar un análisis forense en la nube?

En Colombia no se conoce hasta el momento ninguna norma o procedimiento definido que indique como realizar dicho análisis de los servicios informáticos en la nube.

Esta investigación propone una guía de contratación de servicios en la nube para empresas públicas y privadas en Colombia que garantice un correcto análisis forense cuando se presenten incidentes de seguridad teniendo en cuenta que en la actualidad no existe claridad sobre la correcta manipulación de la información que es compartida con los proveedores de servicios en la nube

2. HIPÓTESIS

El trabajo se abordó bajo la siguiente hipótesis: Se conocen las responsabilidades legales de los proveedores de servicios en la nube y de las empresas que contratan dichos servicios en Colombia, sobre la información que se transfiere a la nube. Así como la forma adecuada de realizar un correcto análisis forense.

3. MARCO DE REFERENCIA

3.1 COMPUTACIÓN EN LA NUBE

El concepto de "computación en la nube" es una nueva tecnología que se basa en el manejo de información en Internet, eliminando los costos asociados al almacenamiento, procesamiento y administración de los datos.

¿Pero qué es Internet?, de acuerdo a la literatura se define como "un conjunto de ordenadores, distribuidos por el mundo y unidos por una tupida malla de comunicaciones, que ofrece espacios de información a todo el que tenga acceso", a lo que se llama nube[1].

La NIST (800-145) define la computación en la nube como: "un modelo que permite el acceso a la red omnipresente y conveniente a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que se puede aprovisionar y liberar rápidamente con un esfuerzo mínimo de gestión o una interacción entre el proveedor de servicios"[2].

De acuerdo a la anterior definición la computación en la nube se describe como una tecnología flexible, que se adapta a las demandas de consumo, donde el usuario no conoce la infraestructura que lo soporta, los servicios son escalables y su nivel de interrupción es casi nulo.

El modelo de computación en la nube se compone de cinco características esenciales, tres modelos de servicio y cuatro implementaciones.

Las características más destacadas son:

Escalable: el crecimiento va de acuerdo a las nuevas necesidades del usuario, sin que eso vaya asociado a nuevos contratos ni penalizaciones.

Accesibilidad: por estar en internet permite un fácil acceso, no requiere estar ligado a una infraestructura, por lo contrario, ofrece la posibilidad del acceso a través de cualquier dispositivo (pc, teléfonos móviles, laptop).

Recursos compartidos. La infraestructura que soporta la tecnología sirve a muchos usuarios de manera controlada y óptima, brindando seguridad en la asignación de recursos. Esto lleva inmerso un sin fin de recursos de almacenamiento, procesamiento, software, y hardware, los cuales son dispuestos para atender las necesidades por demanda de los usuarios, sin que estos tengan conocimiento de su topología y/o ubicación física.

Reducción de costos: ya que no se invierte en infraestructura y los costos asociados a su operación y mantenimiento son trasladados, lo que disminuye sustancialmente la inversión en la administración.

Seguridad: Es considerada aún más seguro que los sistemas tradicionales, ya que las empresas que ofrecen el servicio, destinan gran cantidad de recursos de infraestructura y de personal especializado dedicado a este aspecto.

En la figura 1 se muestra las principales características de las plataformas en la nube.

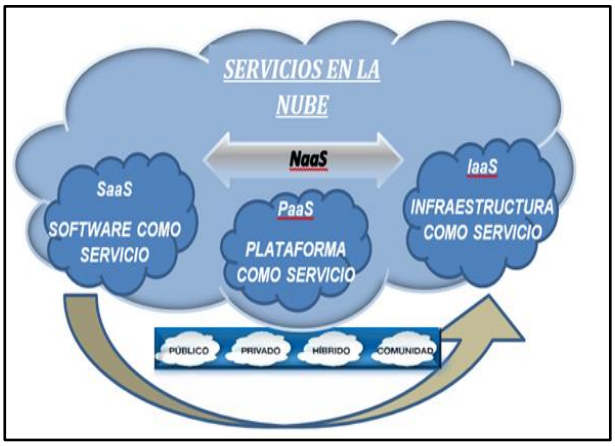


Figura 1. Modelo de computación en la nube

3.2 GESTIÓN DE INCIDENTE

Para determinar un modelo de gestión de incidentes de seguridad se debe definir primero lo que es un evento y un incidente de seguridad.

De acuerdo a la ISO 27001 se define un evento de inseguridad como: “presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad”[3].

Se entiende entonces como evento cualquier alerta producto de una anomalía, o cambio de comportamiento en la infraestructura o componente de un sistema, el cual debe ser gestionado oportunamente antes que produzca un incidente de seguridad. De aquí la importancia del monitoreo de los componentes sensibles o vulnerables en la infraestructura.

Por otra parte, de acuerdo con la misma norma ISO 27001 se denomina incidente de seguridad “un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información”[3].

Entendiendo de esta forma como incidente una violación a las políticas establecidas por una organización, que conlleve o atente contra la integridad, confidencialidad y disponibilidad de la infraestructura que hace parte del sistema de información y de la información misma.

Para lograr un enfoque estructurado, la norma divide la gestión de Incidentes en las siguientes fases de acuerdo con lo que se muestra en la figura 2.

Figura 2. Fases de la Gestión de Incidentes

Teniendo en cuenta lo expuesto en la figura y teniendo en cuenta la estrategia que debe desarrollar la organización para dar cumplimiento al objetivo principal de la gestión de incidentes, la cual es evitar, detectar, contener y eliminar los incidentes de seguridad y así mismo minimizar, eliminar o asumir el impacto negativo

de estos para la organización y relación a los costos directos e indirectos que se causen.

3.3 ANÁLISIS FORENSE DIGITAL

El análisis forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnologías de punta para poder mantener la integridad de los datos y el procesamiento de los mismos, sino que también requiere de una experticia y conocimientos avanzados en materia de informática y sistemas, para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento no solamente del software sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información, etc.

3.4 CONTROLES Y LEGISLACIÓN

Como parte de la investigación se tomaron varios trabajos realizados sobre el aspecto legal de los servicios contratados en la nube y la jurisdicción que los rige.

Las aplicaciones de nube en el sector público y privado comprenden la posibilidad de trastear de la tierra a la nube los datos personales de empleados, clientes y ciudadanos en general. Estos pueden ser almacenados, procesados y administrados por empresas que proveen servicios de nube (CSP). Lo que se haga o no con la información dependerá del contrato que se suscriba.

De acuerdo con el análisis legal de la computación en la nube, la descripción teórica, sus características, esquemas comerciales de ofertas de servicio y tipos de nube evidencian que se trata de una nueva forma de aproximación a la manera en que las personas naturales y jurídicas almacenan información y la comparten.

Frente a este fenómeno en el cual los ordenamientos jurídicos deben ser interpretados y actualizados con el fin de identificar los cuestionamientos o incertidumbres legales que puedan surgir.

Es por esto que el estudio de la computación en la nube debe empezar en la naturaleza legal del servicio y los retos jurídicos que se presentan sobre este tipo de contratos.

Por otra parte, el derecho comparado consiste en el estudio de las diversas instituciones jurídicas a través de las legislaciones positivas vigentes en distintos países.

Dentro de las consideraciones legales también es importante tener claro el concepto del derecho comparado, ya que es necesario realizar un estudio de las diversas instituciones jurídicas a través de las legislaciones positivas vigentes en distintos países.

El derecho comparado se debe enfocar a la investigación restringida a legislaciones de similar afinidad cultural[4].

4. GUÍA DE CONTRATACIÓN DE SERVICIOS EN LA NUBE

A continuación se darán las recomendaciones a tener en cuenta al momento de la contratación de servicios en la nube que garanticen un adecuado manejo para el análisis forense en el momento en que se presente un incidente de seguridad, basados en la norma ISO 27037 e ISO 27042, así como las leyes vigentes de contratación y protección de datos en Colombia.

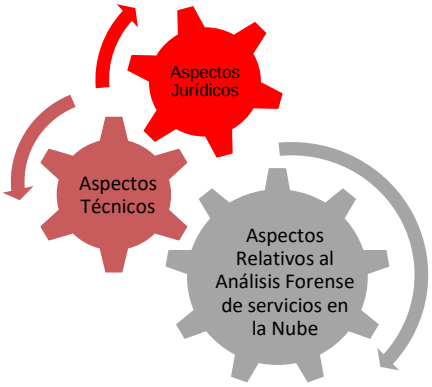


Figura 3. Aspectos Relativos a la contratación en la nube

4.1 ASPECTOS JURÍDICOS

Los mayores retos a nivel jurídico en este tipo de contratación, se presentan en la protección de datos personales, la transferencia internacional de datos, la seguridad de la información almacenada en la nube, las actuaciones criminales, la responsabilidad civil, etc. y el problema de la ley que debe ser aplicada a este tipo de contratos y bajo qué jurisdicción se encuentran.

Las siguientes son las recomendaciones a seguir:

Definir las condiciones de la relación jurídica y la legislación aplicable al contrato, siendo puntual en estipular aspectos de confidencialidad de datos personales y transferencia internacional de datos; el proveedor y los diferentes actores deben garantizar niveles adecuados de seguridad (ley 1581.2012).

Definir el lugar donde estará alojada la información. En caso de que se realice una migración a otro centro de datos o país por cualquier motivo atribuible al proveedor, se debe garantizar que será informado y se deben respetar los acuerdos

establecidos a nivel de políticas de tratamiento de datos personales y legislación mencionados anteriormente.

Realizar el ejercicio de derecho comparado. Teniendo claro las leyes vigentes del estado colombiano en relación al manejo de datos personales, privacidad y transferencia de datos personales, así mismo conocer las leyes vigentes en el (os) país (es) donde estará alojada la información, las cuales deben tener similitud con las de Colombia.

Determinar la distribución de responsabilidades entre los que intervienen en la provisión del servicio al momento en que se requiera realizar una investigación forense. Teniendo en cuenta que en un servicio puede haber un proveedor de la infraestructura física, otro que disponga de los servidores que brinden espacio de almacenamiento y tiempo de procesamiento, otro que monte una plataforma de software como servicio, etc. por esta razón se debe determinar el nivel de participación de cada proveedor.

Definir el alcance jurisdiccional del contrato. Para ello se deben establecer en el contrato acuerdos de cooperación durante la investigación en que el proveedor y los terceros se comprometan en cuanto a la recolección de datos, a su competencia y fiabilidad, los cuales deben ser especificados con claridad en los ANS.

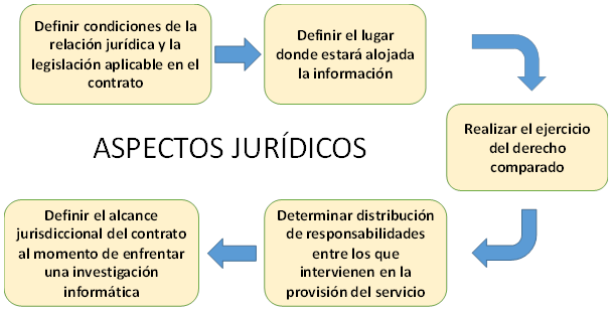


Figura 4. Recomendaciones en el aspecto jurídico

4.2 ASPECTOS TÉCNICOS

Uno de los factores que se deben considerar en el momento de realizar un contrato de servicios en la nube, son los aspectos técnicos en el manejo de un incidente de seguridad, para ello es necesario determinar en primera instancia qué activos tiene la organización, y cuáles de ellos se llevan a la nube. Esto se debe realizar una vez se evalúe el nivel de riesgo asociado que conlleva para la organización, llevar cierta información a un ambiente fuera del ámbito empresarial, en donde el manejo, procesamiento y acceso a la misma será responsabilidad de un tercero.

A continuación, se describen las recomendaciones que se deben contemplar:

Se debe estipular en el contrato los componentes de la arquitectura del servicio y actores de servicio. Así mismo se debe definir que si durante la vigencia del contrato alguno de estos es cambiado o modificado por mejoras o incidentes presentados, o por cambio de terceros o de ubicación de los datos, debe ser comunicado con antelación al contratante, para que de esta forma se de una trazabilidad del servicio por las partes involucradas y en el momento de un incidente que se refiera a un análisis forense, se tenga clara la ubicación y los componentes involucrados en la investigación.

Establecer la propiedad de los datos.

Distribución de responsabilidades ante un incidente de seguridad y tiempo de respuesta ante una investigación forense. Para ello se deben establecer ANS de cumplimiento dentro de contrato.

Manejo de incidentes. Establecer los ANS relativos a la atención de los incidentes de acuerdo a su nivel de impacto. Se debe dar a conocer a la organización contratante la metodología que emplea el proveedor y los actores del servicio para enfrentar un incidente, el control y seguimiento a esta metodología, monitoreo, planes de emergencia, atención, contención y erradicación. Debe quedar definido en el contrato la entrega de informes periódicos de los incidentes presentados, estadísticas, acciones de mejora y de igual forma cuántos de ellos afectaron el servicio contratado. También se deben definir los ANS relativos a la atención de los incidentes conforme a su nivel de impacto.

Debe quedar establecido en el contrato que el proveedor y sus terceros deben evaluar la plataforma de seguridad, garantizando el análisis de vulnerabilidades por lo menos dos veces al año, mecanismos de hardening y re-test. Producto de esto realizara entregas sobre los resultados de estas actividades.

¿Quién accede a los datos? Para ello se debe establecer en el contrato los mecanismos utilizados por los funcionarios del proveedor y sus actores a la infraestructura y la información alojada en ella. Seguridad de contraseñas fuertes (doble factor) y control de acceso. Así mismo, se deben separar los mecanismos de autenticación y credenciales de acceso empleadas por usuarios de la nube a la de usuarios físicos o funcionarios que interactúan con la plataforma.

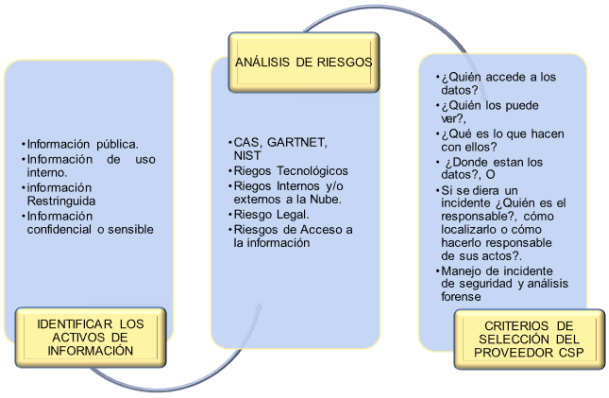


Figura 5. Recomendaciones en el aspecto Técnicos

Se debe informar al proveedor en el momento de la firma del contrato cual es la información que se considerada como sensible para que tenga un manejo diferente, para el caso de un incidente que requiera análisis forense, se de una oportuna respuesta teniendo en cuenta la importancia para la organización.

En el contrato debe quedar estipulado el compromiso del proveedor de servicios en la nube en relación al manejo de la información de bases de datos, servidores, licencias y otras. El incumplimiento de la misma podrá ser causa de acciones civiles y penales aplicables al derecho internacional sobre este aspecto.

4.3 ASPECTOS DEL ANÁLISIS FORENSE DE SERVICIOS EN LA NUBE

A continuación, se describen los aspectos más relevantes del análisis forense, para ello se traerá las normas ISO 27037 (ISO, 2012), ISO 27040 (ISO, 2015) e ISO 27042 (ISO, 2015) y DRAF 8006 (NIST 2014). Estas normas y/o estándares constituyen las mejores prácticas de la informática forense, relacionados con las actividades de identificación, recolección, adquisición, preservación, análisis, interpretación y reporte de incidentes; a su vez se expondrán los problemas y desafíos a que se enfrenta las organizaciones cuando es requerido un análisis forense en la nube.

De acuerdo al análisis anterior se darán a continuación una serie de recomendaciones que es necesario tener en cuenta en el momento de efectuar un contrato con un proveedor de servicio en la nube.

Definir que se permita el acceso a todas las fuentes de análisis forense entre ellas están log, registros de auditorías, registros de seguridad (rastreo de usuarios y acciones), y registros de aplicaciones (errores y fallas operacionales).

Establecer si el proveedor realizar el análisis forense y/o si permite ingresar a un especialista para la reconstrucción del evento y recolección de imágenes virtuales, datos volátiles, metadatos, etc. Si se da el primer caso se debe solicitar en el contrato que el proveedor debe contar con peritos forenses especializados, los cuales deben tener certificaciones internacionales avaladas por las leyes colombianas en esta práctica.

Se debe considerar en este punto que el análisis forense que se requiere estará en la nube, por lo anterior los especialistas deben contar con experiencia en este ambiente.

Se puede definir, en algunas ocasiones, de acuerdo al impacto del incidente, si este análisis forense se puede realizar en forma remota, mediante ejecutables desarrollados para tal fin, y establecer los mecanismos de confiabilidad e integridad de las evidencias recolectadas las cuales serán entregadas por parte del operador y los actores del servicio.

Estipular en el contrato la responsabilidad del proveedor del servicio y sus actores de garantizar que la información vinculante que se encuentre en la nube, no se verá afectada durante un proceso de análisis forense, para ello será el quien determine los procedimientos y metodologías que se emplearan para separar la información vinculante a una investigación forense, sin que ello afecte la confiabilidad e integridad de la recolección y custodia de la evidencia que se requiera y a su vez viole la privacidad de la información de otros usuarios de la plataforma.

Existen algunos componentes a los cuales es difícil llegar y por lo cual no es posible realizar análisis forense en evento que se requiera, estos son los dispositivos finales a través de los cuales son accedidos los recursos de la nube y que no están definidos su ubicación y los cuales no están bajo el dominio de los actores del servicio, es por esto que es necesario que el proveedor tenga un buen procedimiento de control de acceso y seguridad de autenticación y defensa en profundidad.

Figura 6. Recomendaciones para el Análisis Forense

Es importante tener en cuenta que las anteriores recomendaciones de la guía van de acuerdo al tipo de organización contratante y del servicio contratado y no son vinculantes en todo contrato de servicios en la nube.

5. CONCLUSIONES

En el logro de la investigación realizada se puede evidenciar el conocimiento adquirido en los aspectos legales vigentes frente a la contratación de servicios en la nube, así como los aspectos técnicos y forenses que dan como resultado una guía para la contratación de servicios en la nube que garanticen un correcto análisis forense cuando se presente un incidente de seguridad.

De acuerdo al desarrollo de esta guía la organización antes de la selección del proveedor y de la firma del contrato, debe realizar un análisis de riesgos de cada uno de los principales activos de información, como responsable de la misma, y de esta forma determinar cuál de ellos lleva a la nube (privada, pública, hibrida o comunitaria). Para este ejercicio se debe tener en cuenta el impacto implícito frente a los riesgos de la nube; más aún, ahondar cual es el impacto que esto sugiere en caso de requerirse una evidencia digital (económico, prestigio, jurídico). “Mientras mejor conozcamos donde se puede albergar aquella evidencia digital derivada de un incidente en “la nube”, mayor seguridad tendrá la organización para depurar responsabilidad ante un proceso judicial”[5].

Si bien en la actualidad no existen estándares, leyes y/o normas nacionales ni internacionales en las cuales se pueda amparar o sustentar un análisis forense en la nube, ya que la literatura existente soporta esta práctica en los ambientes tradicionales, los desafíos que implica esta actividad en la nube puede considerarse como buen punto de partida para tener en cuenta en el momento de firmar un contrato con un CSP.

El haber realizado el estudio de los estándares dados por la ISO, la NIST y otros estudios elaborados por organizaciones de tecnología y computación en el tema, y analizando cada uno de los desafíos que se

encuentran en la nube frente a seguridad y análisis forense, se entrega como resultado una serie de recomendaciones que facilitan a las empresas Colombianas realizar un contrato que garantice una respuesta adecuada para el análisis forense al momento en que se presente un incidente de seguridad. Una mala definición de los acuerdos en el contrato puede conllevar a la imposibilidad en un futuro, de encontrar la evidencia digital necesaria, para dilucidar responsabilidades, y en consecuencia acarrear perjuicios para la organización de índole económica, civil y penal.

6. REFERENCIAS

[1] MARTÍN, Eduardo. 2014. ¿Qué es 'cloud computing'? Definición y concepto para neófitos. TICbeat. [En línea]. http://www.ticbeat.com/cloud/que-es-cloud-computing-definicion-concepto-para-neofito [citado en 2 de Diciembre de 2014].

[2] MELL, Peter y GRANCE, Timithy. 2014. The NIST Definition of Cloud Computing. National Institute of Standards and Technology. [En línea] <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [citado en 2014].

[3] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. 2006. Tecnología de la información. Técnicas de seguridad. Sitemas de gestión de la seguridad de la información (SGSA). Requisitos. Bogotá: ICONTEC, 2006 (NTC-ISO/IEC 27001).

[4] ENCICLOPEDIA JURÍDICA. S.f. Derecho comparado. Enciclopedia jurídica. [En línea]. <http://www.enciclopedia-juridica.biz14.com/d/derecho-comparado/derecho-comparado.htm> [citado en S.f].

[5] LLEIXÀ I ALSINA, Ángela. 2015. La evidencia digital ante riesgos y amenazas en el Cloud Computing. Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. [En línea]. <http://www.aspectosprofesionales.info/2015/06/la-evidencia-digital-ante-riesgos-y.html> [citado en 6 de Junio de 2015].